Organisering av informasjonssikkerhetsarbeidet i kommuner

Ørnulf Storm

Masteroppgave ved Avdeling for forvaltningsinformatikk

Det juridiske fakultet

UNIVERSITETET I OSLO

August 2009

Forord

Det innføres stadig flere informasjonssystemer som behandler personopplysninger og utfordringene for de behandlingsansvarlige er store. For kommunesektoren, som ofte har trange budsjetter og stor arbeidsbelastning, er det å sikre alle personopplysninger en stor oppgave.

Dersom en kommune kan få hjelp og veiledning til å utføre denne oppgaven kan det kanskje bli enklere. Dersom kommuner hjelper hverandre er det sannsynlig at sikringen av personopplysningene blir bedre. Vi som innbyggere kan da føle oss litt tryggere på at opplysninger om våre personlige forhold, ikke kommer på avveie. Vi kan også være tryggere på at opplysninger om oss som er viktige, ikke blir slettet ved en feil, eller gis til personer som ikke skulle hatt tilgang til dem.

Det har vært en spesiell utfordring å skrive en slik tverrfaglig oppgave. Det å prøve å kombinere juridiske, informatiske og samfunnsvitenskapelige aspekter har ikke vært lett. Jeg har brukt mange rettskilder i oppgaven og det derfor vært spesielt viktig for meg å få veiledning på dette. Jeg har også vært avhengig av å få veiledning på de andre aspektene innen samfunnsvitenskapelige og informatiske forhold. Denne oppgaven har min veileder Dag Wiese Schartum gjennomført på en utmerket måte, og gitt meg den støtten som har vært helt nødvendig for å kunne skrive denne oppgaven. Jeg har også fått gode innspill fra Tommy Tranvik ved utarbeidelse av spørreskjemaet for de semistrukturerte intervjuene.

Jeg vil også takk alle de som stilte opp til intervju i kommunene. Uten dem hadde jeg ikke hatt noe empirisk materiale å analysere.

Jeg vil også til slutt takke Nita for at hun har holdt ut når jeg har brukt kvelder, helger og fridager til å fullføre denne oppgaven.

Arendal, 20. august 2009
Ørnulf Storm

Innholdsfortegnelse

1. Introduksjon til oppgaven og oppgavebeskrivelse

1.1. Hvorfor er organisering av informasjonssikkerhetsarbeid interessant?

Organisering av informasjonssikkerhetsarbeidet kan by på utfordringer. Dette gjelder både hos private og offentlige aktører. Det er ledelsen i en virksomhet som har ansvaret for å sørge for tilfredsstillende informasjonssikkerhet. Flere ulike regelverk setter krav til informasjonssikkerhet[1] og det er flere eksempler på standarder[2] som gir veiledning på hva en skal huske på ved etablering av sikringstiltak i informasjonssystemer. Det er også flere grunner til at en skal sikre informasjonssystemer. Dette kan være å ivareta personvern, økonomiske interesser eller sikre funksjonsdyktighet.[3] Krav til sikring av personopplysninger gis i hovedsak i personopplysningsloven[4] og personopplysningsforskriften.[5] Jeg ønsker å se nærmere krav til informasjonssikkerhet som gjelder behandling av personopplysninger. Det er flere krav til sikring av personopplysninger, og jeg ønsker å se krav i regelverk som har direkte innvirkning på organiseringen av informasjonssikkerhetsarbeidet. Forutsetningen for at rettslige krav kan etterleves, er at ledelsen er klar over sitt ansvar. I denne oppgaven vil jeg undersøke hvordan informasjonssikkerhetsarbeidet blir organisert i kommuner. Jeg ønsker å undersøke dette i kommuner fordi kommuner har en utstrakt kontakt med sine innbyggere. Kommuner behandler veldig mye personopplysninger, og derfor vil det være interessant å se på om sikkerheten rundt disse personopplysningene blir ivaretatt på en god og forsvarlig måte. Kommuner inngår i en parlamentarisk styringskjede som stiller dem ovenfor flere og annerledes utfordringer enn private organisasjoner.[6] Min antagelse er at mange kommuner har begrenset kunnskap om lover og regelverk som setter krav til informasjonssikkerhet. Dette bekreftes i en spørreundersøkelse[7] som er gjennomført av

[1] Jf. Jansen og Schartum 2005.
[2] Som for eksempel NS-ISO/IEC 27002
[3] Jf. Jansen og Schartum 2005 side 13.
[4] Lov av 14. april 2000 nr 31om behandling av personopplysninger (personopplysningsloven).
[5] Forskrift av 15. desember 2000 nr 1265 om behandling av personopplysninger (personopplysningsforskriften)
[6] Jf. Christensen 2004 side 17
[7] TØI rapport 800/2005

Transportøkonomisk institutt[8] (TØI) på oppdrag av tidligere Moderniseringsdepartementet (MOD), nå Fornyings- og administrasjonsdepartementet[9] (FAD) og Datatilsynet[10]. Blant virksomhetene som var med i undersøkelsen var flere kommuner.[11] På bakgrunn av dette har jeg grunnlag for å anta at kommuner ikke tar utgangspunkt i juridiske krav når de jobber med informasjonssikkerhet. Datatilsynet hadde kommunesektoren som ett av sine 3 fokusområder for sin virksomhet i 2003.[12] For å sikre at personopplysninger blir ivaretatt på en forsvarlig måte, har myndighetene gitt regler for hvordan behandling av personopplysninger skal foregå. I vurderingen av hvorvidt kommuner etterlever juridiske krav vedrørende behandling av personopplysninger, ønsker jeg å konsentrere meg om de mest sentrale regelverkene som har regler som gjelder for behandling av personopplysninger. Jeg kunne ha vurdert alle juridiske krav som gjelder generelt for behandling av personopplysninger, men jeg ønsker i min oppgave å se nærmere på kravene som gjelder for sikring av personopplysninger og da nærmere bestemt regler for organisering av informasjonssikkerhetsarbeidet.

1.2. Beskrivelse av grunnleggende begreper og problemstillinger

Jeg nevnte i avsnittet ovenfor at jeg ønsker å konsentrere meg om krav til sikring av personopplysninger i kommuner som har direkte innvirkning på organisering av informasjonssikkerhet. Det er derfor nødvendig å klargjøre hva personopplysninger er. Personopplysninger er definert i personopplysningsloven § 2 nr 1:
personopplysning: opplysninger og vurderinger som kan knyttes til en enkeltperson

Jeg kommer tilbake til virkeområdet til personopplysningsloven senere i oppgaven, men nevner kort at pol § 3 bokstav a sier:

[8] Transportøkonomisk institutt – Stiftelsen Norsk senter for samferdselsforskning, www.toi.no sist besøkt 2. juni 2009.
[9] Fornyings- og administrasjonsdepartementet, http://www.regjeringen.no/nb/dep/fad.html?id=339, sist besøkt 2. juni 2009
[10] Datatilsynet er et uavhengig forvaltningsorgan underlagt Kongen og departementet, http://www.datatilsynet.no/templates/AboutPage____220.aspx, sist besøkt 2,. juni 2009
[11] TØI rapport 800/2005 side 2.
[12] Jf. St. meld. nr. 43 (2003-2004).

Loven gjelder for

a) behandling av personopplysninger som helt eller delvis skjer med elektroniske hjelpemidler

Videre i denne oppgaven vil jeg bruke forkortelsen "pol" for personopplysningsloven. Samtidig så sier personopplysningsforskriften § 2-1 i første setning at reglene i kapittel 2 i personopplysningsforskriften gjelder for behandling av personopplysninger som helt eller delvis skjer med elektroniske hjelpemidler. Jeg vil videre i denne oppgaven bruke forkortelsen "pof" for personopplysningsforskriften. Dette danner grunnlaget for hvilken type informasjon som faller inn under definisjonen personopplysninger og som behandles med elektroniske hjelpemidler, og som deretter er gjenstand for krav til sikring. Pol lister opp flere legaldefinisjoner og to legaldefinisjoner er viktige å merke seg. Pol § 2 nr 4 definerer behandlingsansvarlig:

behandlingsansvarlig: den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes,

og pol § 2 nr 5 definerer databehandler:

databehandler: den som behandler personopplysninger på vegne av den behandlingsansvarlige

Både behandlingsansvarlig og databehandler er sentral i loven. En mer utførlig beskrivelse av hvem som kalles behandlingsansvarlig og databehandler er beskrevet i forarbeidene[13] til pol. Føring på hvem som er behandlingsansvarlig fremgår direkte av legaldefinisjonen i pol § 2 nr 4. Det er den som bestemmer formålet med en behandling av personopplysninger og som bestemmer hvilke hjelpemidler som skal brukes som etter loven er behandlingsansvarlig. Behandlingsansvarlig for en kommune vil være kunne være kommunen ved ordføreren eller kommunen ved rådmannen. Det er først og fremst ordlyden i legaldefinisjonen, den som bestemmer formålet og hvilke hjelpemidler som skal brukes, som er bestemmende for hvem som etter loven er å anse som behandlingsansvarlig. Schartum og Bygrave 2006[14] drøfter hvem som bør defineres som behandlingsansvarlig for virksomheter som er juridiske personer. En kommune er en virksomhet som faller inn under definisjonen juridisk person. For en kommune gjelder

[13] Ot. prp. nr. 92 (1998-99)
[14] Schartum og Bygrave 2006 punkt 2.5.3

forvaltningens generelle interne organisasjons- og instruksjonsmyndighet.[15] Den som er behandlingsansvarlig i en kommune vil derfor kunne delegere oppgaver til underordnet i egen organisasjon. I tillegg til denne generelle organisasjons- og instruksjonsmyndigheten er det i kommuneloven gitt flere særskilte delegasjonshjemler. Det er kommunestyret og ledelsen i kommunene og de kommunale organer i en kommune, som kan ta avgjørelser om organisering av virksomheten og hvilke oppgaver de forskjellige enhetene skal ha.[16] Pol § 13 stiller opp krav til informasjonssikkerhet for en behandlingsansvarlig. En databehandler er en som behandler personopplysninger på vegne av en behandlingsansvarlig.[17] Når personopplysninger behandles elektronisk i informasjonssystemer vil det ved mange tilfeller, som for eksempel av økonomiske grunner, være ønskelig å la andre enn egne ansatte ha oppgaver innen drift og vedlikehold av informasjonssystemer. Dersom et IT-firma gis ansvar for drift av et informasjonssystem og har datamaskiner som lagrer og behandler personopplysninger på vegne av en kommune, vil dette firmaet etter loven kalles en databehandler. Det blir mer og mer vanlig at kommer setter bort hele eller deler av sine IKT-tjenester og dermed benytter seg av en databehandler. Det følger av pol §§ 13 og 15 krav til både den behandlingsansvarlige og til databehandleren. Dette er noe som kommunene må være klar over og være i stand til å håndtere. Kommuner har mulighet for å inngå samarbeid med andre kommuner jf. kommuneloven § 27 og lov om interkommunale selskaper. [18] Noen kommuner har inngått samarbeid etter kommuneloven § 27 om felles IKT-leverandør. I et slikt tilfelle vil kommuner kunne ha et delt behandlingsansvar for personopplysninger, og den felles IKT-leverandøren vil være en databehandler for alle kommunene som har inngått et samarbeid.

Forarbeidene til pol sier at når en snakker om sikring av personopplysninger, er det vanlig særlig å fokusere på tiltak av tekniske og organisatorisk art.[19] Regelverkene som regulerer krav til informasjonssikkerhet spesifiserer noen krav til organisering. Krav til organisering er ikke nødvendigvis beskrevet i detalj. Hvilke tiltak som må gjennomføres

[15] Erik Boe Bind 2 kapittel 41.21.
[16] Jf. kommuneloven.
[17] Jf. pol § 2 nr 5.
[18] Lov om interkommunale selskaper av 29. januar 1999 nr 06.
[19] Jf. Ot. prp. nr. 92 side 71 og NOU 1997:19 side 95.

og hvordan organisering bør gjennomføres, avhenger av hvilken trussel man stor ovenfor og resultatet fra en risikovurdering.[20] Pol sier at det skal sørges for tilfredsstillende informasjonssikkerhet med hensyn på konfidensialitet, integritet og tilgjengelighet, jf. pol § 13. Forarbeidene[21] til pol beskriver at kravet til konfidensialitet skal sikre at informasjon ikke blir gjort tilgjengelig for uvedkommende, og at dette betyr at personopplysninger skal være beskyttet mot uautorisert innsyn under behandlingen, f.eks. ved bruk, transport og lagring. Kravet til integritet går ut på at informasjon ikke skal kunne endres utilsiktet, eller av uvedkommende. Kravet til tilgjengelighet skal sikre at personopplysningene er tilgjengelig for rettmessige brukere, når de har behov for det for å kunne utføre sine oppgaver. Kommentarene til pof sier at begrepet informasjonssikkerhet omfatter sikring av konfidensialitet, integritet og tilgjengelighet og gir en kort definisjon på de tre begrepene.[22] Informasjonssikkerhet er ikke eksplisitt definert i pol eller i pof men det nærmeste en kommer er pof § 2-1 første ledd som sier:

§ 2-1. Forholdsmessige krav om sikring av personopplysninger

Reglene i dette kapittelet gjelder for behandling av personopplysninger som helt eller delvis skjer med elektroniske hjelpemidler der det for å hindre fare for tap av liv og helse, økonomisk tap eller tap av anseelse og personlig integritet er nødvendig å sikre konfidensialitet, tilgjengelighet og integritet for opplysningene.

Overskriften til kapittel 2 i pof er dessuten også informasjonssikkerhet.
Dette sammen med ordlyden i pol § 13 er grunnlaget for hva jeg mener med informasjonssikkerhet i denne oppgaven.

Det kan også være interessant å se hva tekniske standarder definerer informasjonssikkerhet til å være. NS-ISO/IEC 17799[23] gir en generell definisjon av informasjonssikkerhet. Informasjonssikkerhet er her definert til å være ”*Beskyttelse av informasjonens konfidensialitet, integritet og tilgjengelighet*” der konfidensialitet er definert som ”*Å sikre at informasjonen er tilgjengelig bare for dem som har autorisert tilgang*”, integritet definert som ”*Å sikre at informasjonen og behandlingsmetodene er*

[20] Jf. Ot. prp. nr. 92 (1998-99) side 115
[21] Ot. prp. nr. 92 (1998-99) side 114-115.
[22] Personopplysningslovens kommentarutgave side 344.
[23] NS-ISO/IEC 17799:2005, Informasjonsteknologi – Administrasjon av informasjonssikkerhet. ISO/IEC 17799 er nå erstattet av ISO/IEC 27002:2005.

nøyaktige og fullstendige" og tilgjengelighet definert som "*Å sikre autoriserte brukeres tilgang til informasjon og tilhørende resurser ved behov*". Dersom en anser informasjonen som skal beskyttes for personopplysninger, gir denne standarden en ganske lik definisjon av begrepet informasjonssikkerhet som regelverkene har gitt. Dette er interessant fordi det i forarbeider og regelverk er henvisninger til anerkjente metoder for informasjonssikkerhet.

Samtidig er det viktig å ha klart for seg hva som menes med organisering. Forarbeidene[24] til pol i kapittel 9 bruker begrepene tekniske og organisatoriske tiltak. Pol sier at tilfredsstillende informasjonssikkerhet skal oppnås gjennom planlagte og systematiske tiltak, jf pol § 13 første ledd.[25] I kommentarene til pof henvises det også til de planlagte og systematiske tiltak jf. pol § 13, og til at de tiltakene som etableres kan være både organisatoriske, fysiske og tekniske.[26] Det kan også tenkes andre systematiske tiltak. Det sies videre i forarbeidene at sikringskrav vil kunne bedre etterlevelsen av lovgivningen om behandling av personopplysninger ved at de høyner bevissthetsnivået hos de behandlingsansvarlige når de som følge av slike krav må gjennomgå viktige organisatoriske og praktiske forhold ved virksomheten. Jeg vil i denne oppgaven konsentrere meg om de organisatoriske tiltak som inngår direkte i informasjonssikkerhetsarbeidet.
Jeg forstår derfor organisering i denne oppgaven til å være tiltak av organisatorisk art som en kommune har gjennomført for å sikre personopplysninger.

Siden jeg skal gjøre undersøkelser i kommuner er det interessant å se på hvordan de samme begrepene forstås innen organisasjonsteori for offentlig sektor. Ved tolkning av resultater i mine undersøkelser der jeg eventuelt vil kunne bruke organisasjonsteori, er det nyttig å vite om begrepene som brukes i lov og forskrift er noenlunde de samme begrepene som brukes innen organisasjonsteori. I Christensen m.fl. 2004[27] gis det en beskrivelse ut fra et instrumentelt perspektiv av hva som menes med

[24] Ot. prp. nr. 92 (1998-99)
[25] Personopplysningslovens kommentarutgave side 129 slår fast at pol § 13 gjennomfører Europaparlamentes- og rådsdirektiv artikkel 17 nr 1. og 2.
[26] Personopplysningslovens kommentarutgave side 128-133.
[27] Jf. Christensen m.fl. 2004 side 31

organisasjonsstruktur. Her beskrives organisasjonsstruktur som den formelle strukturen som består av posisjoner og regler for hvem som bør eller skal gjøre hva, og hvordan ulike oppgaver bør eller skal utføres. Det instrumentelle synet på organisasjoner finnes igjen i forvaltningsretten. Forvaltningsretten beskriver hvordan offentlige organisasjoner skal styres gjennom lover og regler. Det instrumentelle synet er at organisasjoner er redskaper eller instrumenter som skal oppnå visse mål som er definert av samfunnet som viktige.[28]

Ved organisering av informasjonssikkerhetsarbeidet må en også ta i betraktning tiltak og oppgaver som skal gjennomføres. Den som skal gjøre dette i praksis må en ta hensyn til den eksisterende formelle organisasjonsstrukturen i kommunen, og tilpasse organiseringen av informasjonssikkerhetsarbeidet til dette. Det kan også være at den eksisterende formelle organisasjonsstrukturen må endres, for å tilpasse den til hva som passer best når oppgaver og tiltak innen informasjonssikkerhet tas inn i organisasjonen.

Jeg ønsker i oppgaven min å vurdere om kommunene etterlever rettslige krav om sikring av personopplysninger. Jeg må da først kartlegge den rettslige reguleringen for sikring av personopplysninger. Dette vil være en del av referansegrunnlaget for undersøkelsene i kommunene. Den første problemstillingen i oppgaven min blir dermed:

1) Hvilke rettslige krav gjelder for organisering av arbeidet med å sikre personopplysninger i kommuner?

Rettslige krav kan komme til uttrykk på flere måter. Avtaler som er inngått er rettslig bindene for de partene som har inngått dem. Ved søknad om konsesjon ved behandling av personopplysninger etter pol, jf. pol § 33, vil konsesjonsvilkårene som Datatilsynet fastsetter være av typen rettslige krav. For kommuner vil det ikke være gitt mange konsesjoner fordi de fleste av en kommunes behandling av sensitive personopplysninger vil være hjemlet i lov. De vil dermed være unntatt fra konsesjonsplikten jf. pol § 33 fjerde ledd. Når jeg har klarlagt hvilke rettslige krav som gjelder for sikring av

[28] Jf. Christensen m.fl. 2004 side 30

personopplysninger, vil jeg benytte resultatet som del av referansegrunnlaget for undersøkelsene i kommunene.

På grunn av antagelsen om at kommuner har begrenset kunnskap om regelverk som setter krav til informasjonssikkerhet[29], kan jeg forvente å finne at organiseringen av informasjonssikkerhetsarbeidet har liten kobling til rettslige krav. Ledelsen er muligens ikke alltid klar over sitt ansvar, og det kan være IT-ansvarlige i kommuner som må jobbe og kjempe for at informasjonssikkerhet skal bli tatt alvorlig. En kommunes faktiske organisering vil kunne ha innvirkning på hvordan oppgaver innen informasjonssikkerhetsarbeidet er løst. Selv om bevissthet omkring regelverkene er liten, vil det ikke nødvendigvis være slik at ingen krav som regelverkene stiller, blir etterlevd i praksis. Hvilke andre krav enn de juridiske, som ligger til grunn for organisering av informasjonssikkerhetsarbeidet i kommuner, hadde det vært interessant å få vite noe om. Den neste problemstillingen jeg ønsker å se på er derfor følgende:

2) Hvordan har kommuner organisert informasjonssikkerhetsarbeidet?
    a) Hvordan er informasjonssikkerhetsarbeidet faktisk organisert?
    b) Hva har reelt sett vært styrende for organiseringen av informasjonssikkerhetsarbeidet? (regelverk, instrukser, avtaler, modeller, standarder mv)

Jeg vil undersøke hvem som har fått ansvar og myndighet til å foreta beslutninger. Ved å undersøke mer i dybden vil jeg kunne finne ut bakgrunnen for at ansvars- og myndighetsforhold er etablert. Har ansvars og myndighetsforhold opphav i rettslige krav som beskrevet ovenfor eller finnes det andre årsaker, slik som organets generelle organisasjons- og instruksjonsmyndighet. Det kan også være instrukser som er gitt i kommunene som beskriver interessante forhold.

[29] Jf. TØI rapport 800/2005

Jeg ønsker å undersøke hva som har vært styrende for hvordan organiseringen er gjennomført. Dersom ikke de rettslige kravene har vært styrende, så er det kanskje andre krav eller faktorer som har spilt en rolle. Har andre regelverk som ikke regulerer sikring av personopplysninger spilt en rolle i organiseringen av informasjonssikkerhetsarbeidet? Det vil være interessant dersom de har brukt internasjonale standarder for informasjonssikkerhet som grunnlag.

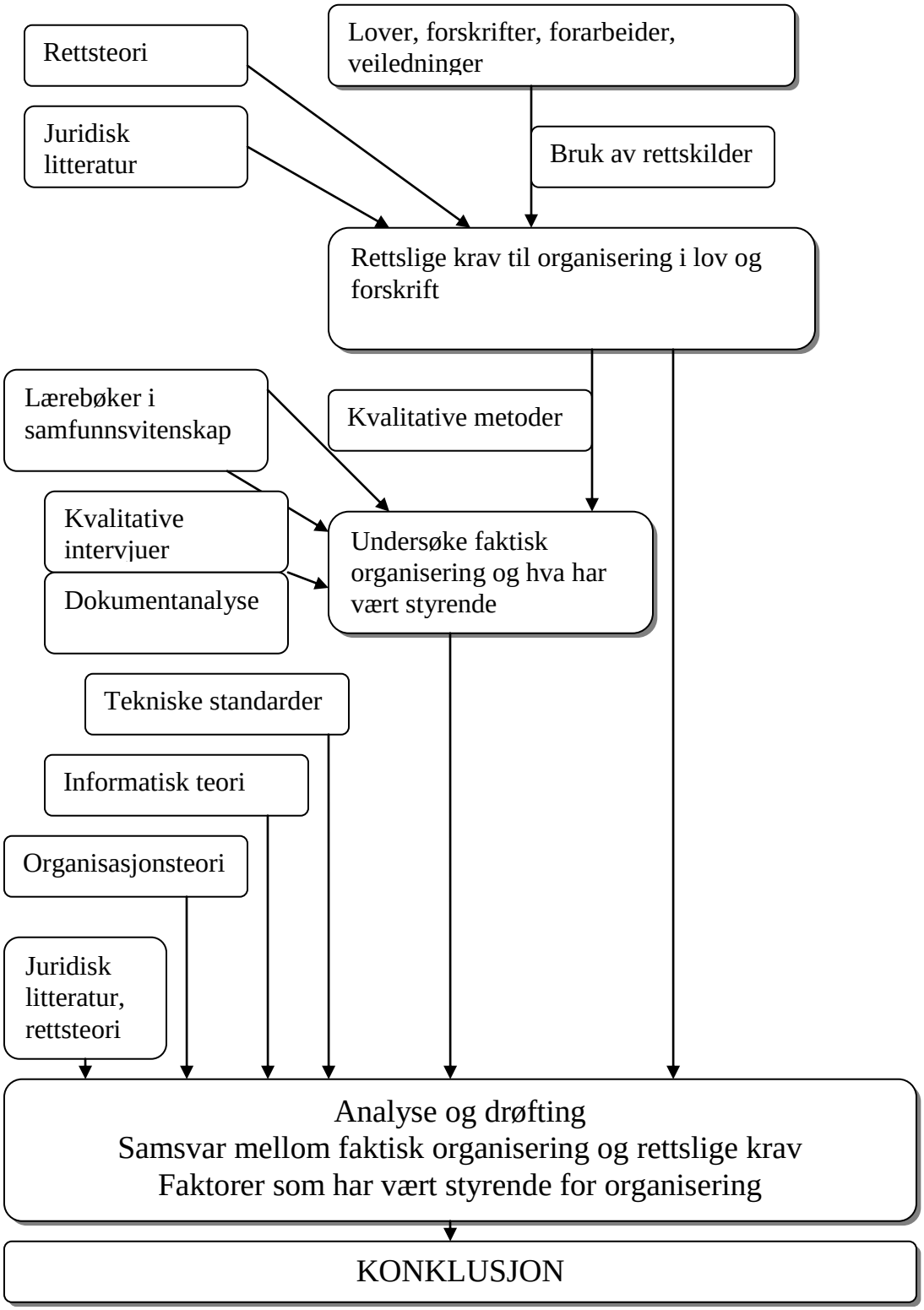
Som jeg har sagt innledningsvis er det interessant å se på om kommuner etterlever rettslige krav. Det siste forholdet jeg derfor ønsker å se på er:

3) Hvilket samsvar er det mellom hvordan organiseringen faktiske er gjennomført og de rettslige kravene?

For å finne ut av hvordan en kommune etterlever de rettslige kravene ønsker jeg ikke å ta for meg paragraf for paragraf og drøfte disse rettsdogmatisk for se om disse etterleves. Jeg vil bruke undersøkelsene der jeg har sett på den faktiske organiseringen og se etter strukturer og aktiviteter og i etterkant sammenligne dette med de rettslige kravene. Til tross for antagelsen om lite kunnskap om regelverk, forventer jeg å finne etterlevelse av krav i regelverk som har opphav i andre faktorer.

1.3. Bruk av metoder

1.3.1. Oversikt over forskningsdesign og metodespørsmål



Figur 1 - Forskningsdesign og bruk av metoder

Denne oppgaven består i første omgang å se på krav i lov og forskrift som regulerer organisering av informasjonssikkerhetsarbeidet. Til dette gjør jeg bruk av rettskilder. Jeg bruker i tillegg spørreordene hvem, hva og hvordan. Jeg kobler hvem til personelle krav, hva til materielle krav og hvordan til prosessuelle krav. Dette forklarer jeg nærmere i kapittel 2. Hva som er rettskilder er beskrevet i juridisk litteratur.[30] Lover, forskrifter, forarbeider, rettsavgjørelser og forvaltningspraksis er eksempler på rettskilder. Lover og forskrifter er tilgjengelige på Internett via Lovdata[31] sine nettsider og herfra har jeg hentet ut alle nødvendige lover og forskrifter. På Internett finnes mye forskjellig informasjon og ved normal informasjonsinnhenting fra Internett må kilden til informasjonen vurderes nøye. Når det gjelder Lovdata er dette en privat stiftelse[32] opprettet av Justisdepartementet og Det Juridiske fakultet ved Universitetet i Oslo. Det er vanlig for jurister og andre i mange samfunnssektorer blant annet advokater, politi- og påtalemyndigheten og offentlig forvaltning.[33] å hente informasjon fra Lovdata. Forarbeider til lover finnes også tilgjengelig på Internett[34], men i tillegg brukte jeg særtrykk for utvalgte odelstingsproposisjoner fra Statens forvaltningstjeneste. Jeg har også søkt i rettsavgjørelser på Rettsdata[35]. Som kilde for juridiske begreper og bruk av rettskilder og begreper fra forvaltningsretten har jeg brukt lærebøker[36] fra juridiske studier, Erik Boe Bind 1.[37] Personvernnemndas vedtak finnes på Internett.[38] Datatilsynets vedtak ovenfor kommuner for 2008 og 2009 som omhandlet informasjonssikkerhet, fikk jeg tilsendt fra Datatilsynet etter en begjæring om innsyn.

Etter å ha studert de rettslige krav har jeg brukt mine funn for å lage et undersøkelsesopplegg for å se på hvordan den faktiske organiseringen av

[30] Erik Boe Bind 1.
[31] www.lovdata.no
[32] Jf. www.lovdata.no/info/fakta.html
[33] Jf. www.lovdata.no/info/info.html
[34] Jf. www.odin.no og søk på odelstingsproposisjoner på det enkelte departement og under hver Ot. prp. søk i sakens dokumenter (ESOP-søk).
[35] Betalingstjeneste på www.rettsdata.no der alle rettsavgjørelser finnes. Her har jeg søkt i databasene etter nøkkelord som har med informasjonssikkerhet og personvern å gjøre. Gyldendal Rettsdata er også en nettbasert rettskildebase som brukes av juridiske miljøer i Norge.
[36] Jf. Erik Boe Bind 2.
[37] Jf. Erik Boe Bind 1
[38] http://www.personvernnemnda.no/vedtak/index.htm

informasjonssikkerhetsarbeidet er gjennomført, og hva som har vært styrende for arbeidet. Fordi jeg ønsker å gå i dybden i problemstillingene, ønsker jeg å gjennomføre kvalitative undersøkelser i kommunene. Jeg ønsker å vite noe om årsaken eller bakgrunn for den faktiske organiseringen av informasjonssikkerhetsarbeidet, og hvilke organisatoriske tiltak som er gjennomført. Dersom jeg hadde brukt kvantitative undersøkelser, hadde jeg nok ikke klart å få tak i den informasjonen jeg er ute etter. For informasjonsinnhentingen i kommunene ønsker jeg å bruke kvalitative intervjuer[39] og nærmere bestemt semistrukturerte intervjuer. Det vil også være hensiktsmessig å gå gjennom relevante kommunale instrukser og dokumenter for å lete etter informasjon. Svakheten med valget av kvalitativ metode er at jeg ikke vil kunne generalisere og si at dette vil gjelde for andre kommuner. Jeg vil kun være i stand til å kunne si noe om forhold i de kommunene jeg undersøker. Jeg vil kunne si noe om hvor gode de gjennomførte organisatoriske tiltakene er og dermed hvordan personvernet for innbyggerne i disse kommunene er ivaretatt. Ved kvalitative undersøkelsene vil jeg kunne bedre forstå bakgrunn for valg og prioriteringer og muligens få innblikk i årsakssammenhenger, som jeg ikke vil kunne klart å identifisere ved en kvantitativ undersøkelse.

Oppgaven vil på bakgrunn av dette ha et klart juridisk perspektiv. Videre i oppgaven vil også de samfunnsvitenskapelige perspektiver fra organisasjonsteori og informatiske/teknologiske aspekter ha innvirkning på det jeg skal se på, både i forbindelse med utforming av spørreundersøkelsen og ved analysen av innsamlet materiale. Jeg vil også der det er hensiktsmessig bruke rettsteori og organisasjonsteori når jeg ser på hva som har vært styrende for organiseringen av informasjonssikkerhetsarbeidet. Jeg mener det er viktig å prøve å få med flere fagområder og perspektiver i en masteroppgave innen forvaltningsinformatikk. Forvaltningsinformatikk er et tverrfaglig fagområde der en arbeider i skjæringspunktet mellom jus, informatikk og samfunnsvitenskap.

[39] Pål Repstad 2007 side 78.

1.3.2. Om bruken av rettskilder i oppgaven

For å kunne undersøke rettsregler som gjelder innen et rettsområde må en bruke ulike rettskilder. For å fastslå gjeldende rett må en tolke det som kalles rettskilder. Lover, forskrifter, forarbeider og etterarbeider til lover, rettspraksis og da særlig høyesterettsdommer, myndigheters praksis og rettsoppfatninger i juridisk litteratur er som ovenfor nevnt rettskildefaktorer. Jeg er ikke jurist og behersker derfor ikke juridisk metode og prøver derfor heller ikke å drøfte gjeldende rett i min oppgave. Jeg bruker ulike rettskilder for å kartlegge hvilke rettsregler som spesielt gjelder for organisering av informasjonssikkerhetsarbeidet. Jeg har tatt utgangspunkt i lovtekstene og forskriftene, og deretter lest relevante forarbeider og veiledninger til forskriftene. Ved gjennomgangen av forskriftene vil det være relevant å se på veiledningene som departementene har gitt til forskriftene. Ved gjennomgang av pof vil det også være relevant å gjennomgå veiledninger som Datatilsynet har skrevet, selv om at det forventes samsvar mellom veiledning som departementet har gitt og eventuelle spesielle veiledninger Datatilsynet har skrevet. Datatilsynet kan gi pålegg om vilkår som må oppfylles for at behandling skal være i samsvar med loven, jf. pol § 46 og det kunne vært av interesse å se på om slike vedtak inneholder noe mer enn det jeg allerede har kategorisert av rettsregler basert på de andre rettskildene. Slike pålegg kan gis som enkeltvedtak jf. pol § 46 fjerde ledd og pof § 2-2. Bruken av slike enkeltvedtak er også beskrevet i Ot. prp. 92[40] (1998-99) og Innst. O. nr 51[41] (1999-2000) kapittel 9. Jeg vil også se på rettspraksis og se om det er noen dommer som berører de rettsreglene jeg har kategorisert. Rettspraksis og da særlig høyesterettsdommer er en viktig rettskilde, men dersom det ikke har vært noen høyesterettsdommer som berører de kjerneområdene som jeg skal se på i denne oppgaven, vil rettspraksis ha mindre betydning for kategoriseringen min. Jeg vil også sjekke om det er noen klagebehandling foretatt av Personvernnemnda[42] som vil kunne ha innvirkning på min kategorisering. Personvernkommisjonens[43] rapport[44] påpeker på at det en høy prosentandel av Datatilsynets vedtak som blir klaget inn for Personvernnemnda,

[40] Ot. prp. nr. 92 (1998-99)
[41] Innst. O. nr 51 (1999-2000)
[42] Jf. personopplysningsloven § 42 fjerde ledd og § 43.
[43] Personvernkommisjonen ble oppnevnt ved kongelig resolusjon 25. mai 2007 for å foreta en utredning om personvern.
[44] NOU 2009:1 side 205

som blir omgjort. Det vil derfor kunne være interessant dersom noen av disse avgjørelsene omhandler sikring av personopplysninger. Jeg vil også bruke relevant juridisk litteratur på området.

1.3.3. Spesielt om bruken av semistrukturerte intervjuer

For den delen av oppgaven der jeg skal gjøre undersøkelser i kommuner må jeg bruke en metode for å gjennomføre et undersøkelsesopplegg. Jeg har allerede antydet at jeg skal bruke kvalitativ metode for å kunne undersøke mer i dybden. Ved en kvalitativ tilnærming vil jeg forhåpentligvis klare å få en helhetlig beskrivelse av en kommunes organisasjon, og klare å få fram en god beskrivelse av prosessene rundt organisering av informasjonssikkerhetsarbeidet. En slik kvalitativ studie vil være egnet for å kunne forstå hvordan en konkret kommune har løst sine oppgaver på. Dette beskrives i metodelitteratur[45] som den beste metoden dersom en ønsker å forstå avgrensede enkeltmiljøer. I figuren ovenfor beskriver jeg at vil benytte meg av dokumentanalyse og semistrukturerte intervjuer. Enkelte opplysninger jeg er ute etter vil være å finne i instrukser og annen skriftlig dokumentasjon. For selve intervjuene har jeg utviklet en intervjuguide der jeg har laget noen hovedspørsmål med mulige oppfølgingsspørsmål.

1.4. Oppbygning av oppgaven

Under problemstillingene i innledningen er det beskrevet totalt tre problemstillinger. Den første problemstillingen som går på

1) Hvilke rettslige krav gjelder for organisering av arbeidet med å sikre personopplysninger i kommuner?

behandles i kapittel 2 der også flere avgrensinger foretas. Den neste problemstillingen som lyder:

2) Hvordan har kommuner organisert informasjonssikkerhetsarbeidet?
    a) Hvordan er informasjonssikkerhetsarbeidet faktisk organisert?

[45] Pål Repstad 2007

b) Hva har reelt sett vært styrende for organiseringen av informasjonssikkerhetsarbeidet? (regelverk, instrukser, avtaler, modeller, standarder mv)

Innsamlingen av informasjon med bakgrunn i problemstillingen ovenfor blir behandlet i kapittel 3. Den siste problemstillingen som jeg definert i oppgaven som lyder:

3) Hvilket samsvar er det mellom hvordan organiseringen faktiske er gjennomført og de rettslige kravene?

blir behandlet i kapittel 4. I kapittel 4 drøfter jeg dessuten også hvilken innvirkning faktorene som er blitt identifisert med bakgrunn i problemstilling 2b har på organisering av informasjonssikkerhetsarbeidet. Jeg gir detter noen oppsummeringer og konklusjoner i kapittel 5.

2. Analyse av rettslige krav knyttet til informasjonssikkerhet i lover og forskrifter

2.1. Oversikt over fremstillingen i kapittel 2

Kapittel 2 inneholder en analyse av rettslige krav knyttet til informasjonssikkerhet i relevante lover og forskrifter. Det er nødvendig å gi en kort oversikt over rettslig krav til sikring av personopplysninger først, for så å kunne foreta en nærmere vurdering av hvilke lover som er relevante å ta med i denne analysen. Det blir også gitt en introduksjon til opplegget for identifisering og analyse av de rettslige kravene.

2.2. Oversikt over rettslige krav til sikring av personopplysninger i kommunal forvaltning

2.2.1. Rettslige krav til sikring av personopplysninger

Hovedregelverket som gjelder for behandling av personopplysninger er personopplysningsloven. Loven gjelder for alle behandlinger av personopplysninger som helt eller delvis skjer med elektroniske hjelpemidler, jf. saklig virkeområde i pol § 3 første ledd bokstav a. Loven gjelder derfor for all elektronisk behandling av personopplysninger i en kommune. For at en behandling av personopplysninger skal være lovlig, må kravene i pol § 8 være oppfylt. Dersom sensitive personopplysninger behandles må også pol § 9 være oppfylt. Samtidig må kravene i pol § 11 være tilfredstilt. Dette er også kalt grunnkrav[46] til behandling av personopplysninger. Pol § 8 og § 9 stiller opp at det må finnes et rettslig grunnlag for å behandle personopplysninger. Jeg vil ikke uttype dette ytterligere annet å si at det finnes ulike rettslige grunnlag for å behandle personopplysninger. En beskrivelse av disse krav gis også i kommentarene[47] til pol. Et rettslig grunnlag kan være at det er hjemmel i lov jf. pol § 8 annen setning, eller det kan være å utøve offentlig myndighet jf. pol § 8 bokstav e. For å behandle sensitive personopplysninger må vilkår i pol § 8 være oppfylt, samtidig med at krav i medhold av

[46] Schartum og Bygrave 2004 side 130-142.
[47] Personopplysningslovens kommentarutgave

pol § 9 er oppfylt. Dette kan for eksempel være at den registrerte samtykker i en slik behandling jf. pol § 9 bokstav a. Det er også et krav til at formålet med en behandling skal angis, og at behandlingen kun omfatter det angitte formålet jf. pol § 11 bokstavene b og c. Summen av disse kravene danner forutsetningen som må foreligge, for at en kommune i det hele tatt har lov til å behandle personopplysninger i sine informasjonssystemer.

Krav til sikring av personopplysninger finnes i pof § 13 som lyder:

§ 13. Informasjonssikkerhet

Den behandlingsansvarlige og databehandleren skal gjennom planlagte og systematiske tiltak sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger.

For å oppnå tilfredsstillende informasjonssikkerhet skal den behandlingsansvarlige og databehandleren dokumentere informasjonssystemet og sikkerhetstiltakene. Dokumentasjonen skal være tilgjengelig for medarbeiderne hos den behandlingsansvarlige og hos databehandleren. Dokumentasjonen skal også være tilgjengelig for Datatilsynet og Personvernnemnda.

En behandlingsansvarlig som lar andre få tilgang til personopplysninger, f.eks. en databehandler eller andre som utfører oppdrag i tilknytning til informasjonssystemet, skal påse at disse oppfyller kravene i første og annet ledd.

Kongen kan gi forskrift om informasjonssikkerhet ved behandling av personopplysninger, herunder nærmere regler om organisatoriske og tekniske sikkerhetstiltak.

Her nevnes planlagte og systematiske tiltak som skal sørge for tilfredsstillende informasjonssikkerhet. Hva disse systematiske tiltakene var jeg inne på i kapittel 1. Utredningen et bedre personvern peker på at når det gjelder sikring av personopplysninger, er det vanlig å fokusere på tiltak av tekniske og organisatoriske art.[48] Forarbeidene til pol refererer nettopp også til at NOU 1997:19 sikter til regler om tiltak av tekniske og organisatorisk art.[49] Forarbeidene nevner eksempler på organisatoriske tiltak kan være å etablere klare ansvars- og myndighetsforhold i organisasjonen og sørge

[48] NOU 1997:19 side 95
[49] Jf. Ot. prp. nr. 92 (1998-99) side 71.

for tilfredsstillende kompetanse hos den behandlingsansvarliges personell.[50] Pol § 13 fjerde ledd gir hjemmel for å gi forskrift om informasjonssikkerhet og det er gitt regler for informasjonssikkerhet i kapittel 2 i pof. Pof § 2-1 er sentral i kapittelet og lyder:

§ 2-1. Forholdsmessige krav om sikring av personopplysninger

Reglene i dette kapittelet gjelder for behandling av personopplysninger som helt eller delvis skjer med elektroniske hjelpemidler der det for å hindre fare for tap av liv og helse, økonomisk tap eller tap av anseelse og personlig integritet er nødvendig å sikre konfidensialitet, tilgjengelighet og integritet for opplysningene.

Der slik fare er til stede skal de planlagte og systematiske tiltakene som treffes i medhold av forskriften, stå i forhold til sannsynligheten for og konsekvens av sikkerhetsbrudd.

Et viktig moment er at de planlagte og systematiske tiltakene skal være forholdsmessige og stå i forhold til sannsynligheten og konsekvensen av sikkerhetsbrudd. Det vil derfor ikke være en fasit på hvordan sikkerhetstiltak skal gjennomføres. Det må gjøres en konkret vurdering for hver enkelt behandling av personopplysninger. Hele grunnlaget for organisering av informasjonssikkerhet ligger i at det er gitt regler for sikring av personopplysninger. Uten disse overordnede kravene hadde det heller ikke vært grunnlag for å se på krav til organisering.

På grunn av at jeg har valgt å se på kommuner vil forvaltningsloven[51] med forskrifter være relevant, fordi forvaltningsloven gjelder for alle forvaltningsorganer jf. lovens generelle virkeområde forvaltningslovens § 1, som i denne loven er et hvert organ for stat eller kommune, jf. forvaltningsloven § 1 annet punktum. Forvaltningsloven setter krav til taushetsplikt for blant annet noens personlige forhold, jf forvaltningsloven § 13 første ledd nr 1. Forvaltningsloven § 13c stiller opp et krav til at forvaltningsorganet skal oppbevare dokumenter og annet materiale som er underlagt taushetsplikt på en betryggende måte jf. forvaltningsloven § 13c annet ledd. Her inngår noens personlige forhold jf. forvaltningsloven § 13. Begrepet noens personlige forhold er en egen kategori opplysninger som ikke uten videre kan sammenlignes med pol sin definisjon av

[50] Jf. Ot. prp. nr 92 (1998-99) side 115.
[51] Lov 10. februar 1967 nr 00 om behandlingsmåten i forvaltningssaker (forvaltningsloven).

personopplysninger, jf. pol § 2 nr 1.[52] Forholdet mellom disse to begrepene er nærere drøftet i juridisk litteratur og det nevnes at det er nærliggende å forstå noens personlige forhold som en underkategori av personopplysninger.[53] Siden det er såpass nær kobling mellom disse to begrepene anser jeg forvaltningslovens krav til sikring av opplysninger om noens personlige forhold som relevant i forhold til oppgaven min. Det er derfor også relevant å se på forskrifter gitt med hjemmel i forvaltningsloven, som inneholder krav til sikring av personopplysninger.

En forskrift som er gitt med hjemmel i forvaltningsloven som er av interesse er eForvaltningsforskriften[54]. Eforvaltningsforskriften er gitt med hjemmel i forvaltningsloven § 15a og med hjemmel i esignaturloven[55].
Formålet med eforvaltningsforskriften slås fast i § 1 nr 1. Dette er å legge til rette for sikker og effektiv bruk av elektronisk kommunikasjon med og i forvaltningen. Her nevnes sikker bruk og det gir meg en pekepinn på at denne forskriften er relevant for oppgaven min. Forskriften gjelder dessuten for *elektronisk kommunikasjon med forvaltningen og for elektronisk saksbehandling og kommunikasjon i forvaltningen når ikke annet er bestemt i lov eller i medhold av lov*, jf. § 1 nr 2. Det vil si at den gjelder for alle borgere sin kommunikasjon til en kommune og kommunikasjon fra en kommune og til borgere. I tillegg vil den gjelde for all elektronisk saksbehandling i en kommune og kommunikasjon internt i en kommune og all kommunikasjon som en kommune har med andre forvaltningsorganer. Eforvaltningsforskriften refererer også direkte til pol § 13 og pof kapittel 2 jf. eforvaltningsforskriften § 13 nr 3 bokstav g. Jeg ønsker derfor å ta denne forskriften med videre i min gjennomgang av rettslige krav.

Det fins også annen lovgiving som generelt regulerer rettslige krav til informasjonssikkerhet, men virkeområdet for disse omfatter ikke kommuner. Mer info

[52] Schartum 2007 side 238.
[53] Schartum 2007 side 240.
[54] Forskrift 25. juni 2004 nr. 988 om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften).
[55] Lov om elektronisk signatur (esignaturloven) av 15. juni 2001 nr 81.

om annet regelverk finnes blant annet i Jansen og Schartum 2005.[56] Jeg har kun kommentert det som jeg mener er relevant å kommentere i denne oppgaven.

2.3. Om opplegget for identifisering og analyse av rettslige krav

For å svare på problemstilling nr 1 trenger jeg en metode for å gjøre dette på en systematisk måte. Tilnærmingen til problemstillingen som jeg ønsker å bruke her er å prøve å kategorisere rettsreglene. Rettsregler i forvaltningsretten[57] kan deles inn i primærregler, sanksjonsregler, handlingsregler, beslutningsregler, pliktregler og kompetanseregler. En kan også prøve å skille rettsregler fra hverandre ved enkelt å dele de inn i personelle, materielle og prosessuelle regler.[58] Jeg går ikke inn på en juridisk drøfting av generell kategorisering av rettsregler eller forvaltningsrettens forståelse av personell, materiell og prosessuell kompetanse. Jeg velger helt enkelt å kalle regler om hvem som skal gjøre noe for personelle regler, regler for hva som skal gjøres for materielle regler og hvordan noe skal gjøres for prosessuelle regler. Når jeg går gjennom lover og forskrifter med den hensikt å kategorisere rettsreglene, vil jeg helt enkelt bruke spørreordene, hvem, hva og hvordan. Som nevnt i innledningen i kapittel 1 så defineres formell organisasjonsstruktur i organisasjonsteori som den strukturen som består av posisjoner og regler for hvem som bør eller skal gjøre noe, hva disse skal gjøre, og hvordan ulike oppgaver bør eller skal utføres. Her brukes også hvem, hva og hvordan og jeg mener derfor at det er hensiktsmessig å bruke disse spørreordene ved kategoriseringen av rettsreglene.

Med personelle krav sikter jeg i oppgaver her til hvem som er beskrevet i regelverkene. Dette kan være hvilket organ som skal gjøre noe, eller en tjenestemann i et organ. Det vil kanskje ikke bety så mye om bare organet er identifisert i et regelverk, fordi innen kommunesektoren gjelder som ovenfor også nevnt intern instruksjonsmyndighet.[59] Organet, og i tilfelle for denne oppgaven en kommune, vil normalt kunne delegere gjennomføring av en oppgave til personer i egen organisasjon som følge av denne interne

[56] Jansen og Schartum 2005 side 100-102
[57] Erik Boe Bind 1 side 39-42
[58] Erik Boe Bind 1 side 42-43 og Erik Boe Bind 2 kapittel 38-43
[59] Erik Boe Bind 2 kapittel 41.21

organisasjons- og instruksjonsmyndigheten. Til tross for det er det interessant å se om regelverkene griper inn i denne myndigheten hvert organ i utgangspunktet har. Dette innebærer at organet har myndighet til å foreta endringer i egen organisasjon, uten særskilt hjemmel i lov eller forskrift, og til å delegere oppgaver nedover i egen organisasjon. Samtidig er det i kommuneloven[60] gitt særskilte delegasjonshjemler som regulerer myndighetsforhold mellom kommunestyret i forhold formannskap[61], ordfører[62], administrasjonssjef [63], interkommunale selskap[64] og utvalg[65] mv.

Med materielle krav sikter jeg til oppgaver som er beskrevet i regelverkene. For disse kan en bruke spørreordet hva skal gjøres, og som vil identifisere oppgaver.
De materielle kravene vil være oppgaver innen informasjonssikkerhet som har betydning for organisering. Hvilke oppgaver som skal gjennomføres vil ved en del tilfeller være gitt i lov og forskrift. De materielle rettsreglene har direkte eller indirekte sammenheng med de personelle rettsreglene. Oppgavene som kommunene skal utføre kan være direkte koblet opp mot stillinger i kommunen. De kan også være eller indirekte koblet mot kommunen som virksomhet.

Med prosessuelle krav sikter jeg her til hvordan de materielle oppgavene skal utføres. Lov og forskrift kan utpekte bestemte stillinger til å utføre en bestemt oppgave eller gjennomføre tiltak. Det vil kunne være identifisert både personelle rettsregler, hvem som skal utføre noe, og materielle rettsregler, hvilke sikkerhetsoppgaver som skal utføres. Det vil da også kunne være regler som går på hvordan disse sikkerhetsoppgavene eller tiltakene skal utføres. Dette vil være det jeg i denne oppgaven kaller for prosessuelle rettsregler. Prosessuelle regler vil kunne ha mye å si for organiseringen av informasjonssikkerhetsarbeidet, fordi reglene vil kunne gi detaljer om hvordan de materielle kravene skal utføres. Dette vil kunne ha stor innvirkning på hvordan informasjonssikkerhetsarbeidet faktisk må organiseres.

[60] Lov om kommuner og fylkeskommuner (kommuneloven) av 25. september 1992 nr 107
[61] Jf. kommuneloven § 8 nr 3
[62] Jf. kommuneloven § 9 nr 5
[63] Jf. kommuneloven § 23 nr 4
[64] Jf. kommuneloven § 27 nr 1
[65] Jf. kommuneloven § 10 nr 4

For å svare på problemstillingen: ”Hvilke rettslige krav gjelder for organisering av arbeidet med å sikre personopplysninger i kommuner?”, vil jeg studere rettsreglene som gjelder sikring av personopplysninger i de regelverkene som jeg mener er viktigst å se på. Dette har jeg vært inne på i innledningen til dette kapittelet og jeg vil derfor ta utgangspunkt i pol, pof, forvaltningsloven og eForvaltningsforskriften. Jeg vil gå gjennom hvert regelverk og plassere de forskjellige rettsreglene inn i de 3 ovennevnte kategoriene. Kategori 1 vil inneholde alle som har fått eller kan få tildelt myndighet eller oppgaver, kategori 2 inneholde alle tiltak og oppgaver innen informasjonssikkerhetsarbeidet, og kategori 3 inneholde alle beskrivelser av hvordan de ulike tiltak eller oppgaver skal utføres. Selv om jeg her i utgangspunktet ønsker å plassere alle rettsreglene som gjelder for informasjonssikkerhet i de 3 kategoriene, er det ikke sikkert at alle kategoriene har like stor innvirkning på hvordan organiseringen av informasjonssikkerhetsarbeidet skal gjennomføres på. Dette vil jeg komme tilbake til etter at kategoriseringen er gjennomført.

Kategori 1	Personelle krav	Hvem er tildelt myndighet eller oppgaver innen informasjonssikkerhetsarbeidet?
Kategori 2	Materielle krav	Hva slags tiltak og oppgaver er beskrevet for informasjonssikkerhetsarbeidet?
Kategori 3	Prosessuelle krav	Hvordan skal tiltak og oppgaver i informasjonssikkerhetsarbeidet utføres?

Tabell 1 – Oversikt over kategorier av rettsregler som har betydning for organisering av informasjonssikkerhetsarbeidet.

2.3.1. Generelt om inndeling i personelle, prosessuelle og materielle krav

Gjennomgangen av regelverkene resulterte i 4 tabeller som er vedlagt som Vedlegg 1-4. Disse danner utgangspunktet for mine drøftelser videre i dette kapittelet. Gjennomgangen her skal svare på den første problemstillingen i oppgaven: *Hvilke rettslige krav gjelder for organisering av arbeidet med å sikre personopplysninger i kommuner?* Ved gjennomgangen og inndelingen i de tre kategoriene, var det relativt lett å identifisere de

personelle rettsreglene. Flere steder i både pol og pof er det regler som identifiserer hvem som skal gjøre noe. Detaljer rundt personelle rettsregler gis i avsnitt 2.4. Ved gjennomgangen av forvaltningsloven og eForvaltningsforskriften, er det flere personelle rettsregler og i all hovedsak refererer til ”forvaltningsorganet”[66] eller ”vedkommende forvaltningsorgan”.[67] Andre steder refereres det til ”enhver som utfører tjeneste eller arbeid for et forvaltningsorgan”[68]. Det refereres også til ”innehaver av signaturfremstillingsdata”[69] som er en underkategori av ”enhver som utfører tjeneste eller arbeid for et forvaltningsorgan”.

Ved inndeling i prosessuelle og materielle rettsregler støtte jeg på noen utfordringer. Noen steder var det vanskelig å bestemme seg for hvilken av de to kategoriene de hørte hjemme under. Noen steder er de materielle og prosessuelle reglene litt vevd inn i hverandre. Ett eksempel er i pol § 13 annet ledd første punktum. Å dokumentere informasjonssystemet har jeg kategorisert som en prosessuell regel. Dette er fordi det refereres til at ”det å dokumentere informasjonssystemet”, er en oppgave som skal gjøres, for å oppnå tilfredsstillende informasjonssikkerhet. Samtidig mener jeg at kravet om at informasjonssystemet skal dokumenteres er en materiell regel, fordi det er en oppgave som skal gjøres. Når jeg går gjennom tabellene med hensyn på materielle rettsregler, ser jeg at det er identifisert en god del oppgaver og tekniske tiltak som lov og forskrift pålegger. Dette er oppgaver innen informasjonssikkerhetsarbeidet som skal gjennomføres, men for mange av disse oppgavene mener jeg har liten innvirkning på hvordan organiseringen av informasjonssikkerhetsarbeidet skal gjennomføres på. Det stiller seg litt annerledes for de prosessuelle reglene. For flere av de prosessuelle reglene, gis det detaljer på hvordan oppgaver skal gjennomføres, som kan ha både direkte og indirekte innvirkning organiseringen av informasjonssikkerhetsarbeidet. Det er ikke det at de materielle reglene ikke har noe å si, men jeg mener de har mindre betydning for organisering av informasjonssikkerhetsarbeidet, i forhold til både de personelle og

[66] Jf. forvaltningsloven § 13 bokstav c annet ledd og mange paragrafer i eForvaltningsforskriften; § 4 nr (2), (3), (4), § 5 nr (3) m.fl. For fullstendig liste over referanser til personelle krav i forvaltningsloven og eForvaltningsforskriften, se vedlegg 3 og 4.
[67] Jf. forvaltningsloven § 13 bokstav c første ledd
[68] Jf. forvaltningsloven § 13 første ledd nr 1, § 13 bokstav f første ledd f. fl.
[69] Jf. eForvaltningsforskriften § 20 og § 23.

prosessuelle rettsreglene. De materielle reglene omfatter som nevnt blant annet alle tekniske tiltak.
Det å kartlegge implementering av alle tekniske tiltak i en kommune ville dessuten egnet seg bedre for en kvantitativ studie. En kvantitativ studie ville ikke gitt meg så mye informasjon om hva som hadde vært styrende for hvordan organiseringen av informasjonssikkerhetsarbeidet var gjennomført på. Jeg vil derfor i mine drøftelser videre i dette kapittelet konsentrere meg om de personelle og de prosessuelle kravene.

Jeg beskriver grunnlaget for at det i det hele tatt finnes en organisering av informasjonssikkerhetsarbeidet i kommuner i avsnitt 2.2.1. Her slår jeg fast krav til sikring av personopplysninger i pol § 13 med forskriftshjemmelen i pol § 13 fjerde ledd, som legger grunnlaget for videre detaljering av rettsregler i blant annet pof kapittel 2.

2.3.2. Om rettskildebruken knyttet til kartleggingen av de rettslige kravene

Jeg foretok en grovkategorisering ved gjennomgang av lovtekster og forskrifter. For å bestemme den endelige plasseringen av reglene i de 3 kategoriene gikk jeg gjennom de andre rettskildene, og så om disse gav grunnlag for en annerledes plassering. I drøftingen av de identifiserte rettsreglene så brukte jeg lovforarbeider, veiledninger til forskriftene samt lov og forskrift. Jeg så også på forvaltningspraksis hos Datatilsynet. Jeg brukte her vedtak[70] som Datatilsynet har foretatt ovenfor kommuner i 2008 og 2009. Se for øvrig kapittel 1.3.2 der jeg beskriver bruk av rettskilder.

2.4. Personelle krav

2.4.1. Nærmere om personelle krav

De personelle rettsreglene sier altså noe om hvem eller hvilken stilling i et organ som har fått myndighet. Jeg vil nå se på tabellene i vedlegg 1-4 etter personelle rettsregler. Jeg vil ikke kommentere alle, men konsentrere meg om de jeg anser som viktigst og de som har mest betydning for organisering av informasjonssikkerhetsarbeidet. I pol § 2 nr 4 defineres behandlingsansvarlig og i pol § 2 nr 5 defineres databehandler. Siden begge disse er helt sentrale gjentar jeg legaldefinisjonene her.

[70] Jf. liste over enkeltvedtak foretatt av Datatilsynet ovenfor kommuner i 2008 og 2009

Pol § 2 nr 4: *behandlingsansvarlig: den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes.*

Pol § 2 nr 5: *databehandler: den som behandler personopplysninger på vegne av den behandlingsansvarlige*

Behandlingsansvarlig og databehandler nevnes i flere av de etterfølgende paragrafene pol og pof nevner også den behandlingsansvarlige flere ganger. Dette gjøres i pof § 2-4 annet ledd, § 2-15 første, annet, fjerde og femte ledd, § 3-1 første og annet ledd. Siden pol § 13 også er helt sentral gjengir jeg også denne i sin helhet på nytt her:

Den behandlingsansvarlige og databehandleren skal gjennom planlagte og systematiske tiltak sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger.

For å oppnå tilfredsstillende informasjonssikkerhet skal den behandlingsansvarlige og databehandleren dokumentere informasjonssystemet og sikkerhetstiltakene. Dokumentasjonen skal være tilgjengelig for medarbeiderne hos den behandlingsansvarlige og hos databehandleren. Dokumentasjonen skal også være tilgjengelig for Datatilsynet og Personvernnemnda.

En behandlingsansvarlig som lar andre få tilgang til personopplysninger, f.eks. en databehandler eller andre som utfører oppdrag i tilknytning til informasjonssystemet, skal påse at disse oppfyller kravene i første og annet ledd.

Kongen kan gi forskrift om informasjonssikkerhet ved behandling av personopplysninger, herunder nærmere regler om organisatoriske og tekniske sikkerhetstiltak.

Siden behandlingsansvarlig og databehandler er viktige er det naturlig å starte med disse to. Spesielt behandlingsansvarlig er helt sentral i forhold til organiseringen av informasjonssikkerhetsarbeidet i en kommune. Behandlingsansvarlig beskrives i pol § 13 som den som har ansvaret for å sørge for tilfredsstillende informasjonssikkerhet. Dette påpekes dessuten også i forarbeidene.[71] Forarbeidene[72] sier også at tilfredsstillende informasjonssikkerhet forutsetter blant annet etablering av både organisatoriske og tekniske sikkerhetstiltak. Behandlingsansvarlig er mest sentral fordi det er denne som både bestemmer formålet med en behandling av personopplysninger og hvilke hjelpemidler som skal brukes. Jeg velger å kalle både behandlingsansvarlig og

[71] Jf. Ot. prp. nr 92 (1998-99) side 115
[72] Jf. Ot. prp. nr 92 (1998-99) side 114

databehandler for aktører. Juridisk litteratur kaller de som er identifisert i regelverkene som gjør noe for roller.[73] Jeg bryter ikke direkte med denne inndelingen men velger å dele inn litt annerledes. Jeg bruker også begrepet rolle men da innenfor en behandlingsansvarlig sin egen organisasjon. En rolle identifiserer at det er noen som skal gjøre noe, uten at det nødvendigvis helt konkret er spesifisert hvilken konkret stilling eller person som skal gjennomføre en oppgave. I noen tilfeller vil annet regelverk være med på å identifisere en bestemt stilling. Min forståelse av at hos den behandlingsansvarlige vil det kunne finnes flere roller. Dette er den samme forståelsen som hos Schartum og Bygrave 2006.[74] En databehandler er utenfor en behandlingsansvarligs organisasjon og ved å bruke begrepet aktør er dette med på å presisere at en databehandler ikke er en del av en behandlingsansvarlige sin organisasjon. For forholdet mellom en behandlingsansvarlig og en databehandler er det vanlig å betrakte behandlingsansvarlig som en oppdragsgiver som betaler for et oppdrag utført av et firma, som da er en databehandler. At databehandlere er eksterne er også beskrevet i juridisk litteratur.[75] Det er nettopp også derfor det i pol § 15 gis bestemmelser om at det skal inngås en avtale mellom den behandlingsansvarlige og en databehandler fordi den behandlingsansvarlige ikke kan instruere databehandleren eller personell hos denne. Måten den behandlingsansvarlige sørger for at krav til sikring av personopplysninger blir fulgt, er å sørge for en avtale med databehandleren jf. pol § 15 første ledd og at avtalen innholder etterlevelse av krav til sikring av personopplysninger jf. pol § 15 annet ledd. Den behandlingsansvarlige blir da en aktør som kan ha flere ulike roller knyttet til informasjonssikkerhetsarbeidet. Daglig leder jf. pof § 2-3 og medarbeider jf. pof § 2-8 kaller jeg derfor rolle slik som også det gjøres i juridisk litteratur.[76]

Den behandlingsansvarlige er som ovenfor nevnt den som bestemmer formålet med en behandling av personopplysninger og hvilke hjelpemidler som skal brukes. Dette er utgangspunktet for å fastslå hvem som er behandlingsansvarlig. Forarbeidene til pol sier at dersom den behandlingsansvarlige er en juridisk person vil den behandlingsansvarlige

[73] Jf. Jansen og Schartum 2005 side 109-114
[74] Jf. Schartum og Bygrave 2006 avsnitt 2.5.7
[75] Personopplysningslovens kommentarutgave side 136.
[76] Jansen og Schartum 2005 side 112-113.

være representert ved virksomhetens ledelse[77]. Forarbeidene sier videre[78] her at det bare er subjekter som har sivilprosessuell partsevne – dvs. den som kan opptre som saksøkt i en tvist for domstolene, som kan være behandlingsansvarlig. Kommuneloven § 9 nr 3 annet punktum sier:

Ordfører og fylkesordfører leder møtene i kommunestyret og fylkestinget, formannskapet og fylkesutvalget. Han eller hun er rettslig representant for kommunen og fylkeskommunen og underskriver på dennes vegne i alle tilfelle hvor myndigheten ikke er tildelt andre.

Ordføreren er derfor normalt kommunes rettslige representant dersom myndigheten ikke er tildelt andre, og det vil kunne være kommunen ved ordføreren som er definert som behandlingsansvarlige i en kommune. Dette er kanskje mest utbredt i små kommuner der ordføreren har mulighet for å bestemme formålet med en behandling av personopplysninger. I større kommuner vil det nok ikke være naturlig at det er ordføreren som er behandlingsansvarlig, fordi de ikke er de som bestemmer formålet for diverse behandlinger av personopplysninger. Ved mange behandlinger av personopplysninger, både i små og store kommuner, vil det være rådmannen som er den som bestemmer formålet med en behandling og hvilke hjelpemidler som skal brukes. Av dette følger det at det er kommunen ved rådmannen som ofte er behandlingsansvarlig. Schartum og Bygrave 2006 har drøftet definisjonen behandlingsansvarlig og noen svakheter ved denne definisjonen.[79] Dersom jeg ser på enkeltvedtak[80] foretatt av Datatilsynet, så blir noen ganger kommunen[81] omtalt som behandlingsansvarlig, noen ganger kommunen[82] ved rådmannen som behandlingsansvarlig og noen ganger blir rådmannen[83] ansett å være behandlingsansvarlig. Dersom det er rådmannen som er behandlingsansvarlig blir det mest presist å si at det er kommunen ved rådmannen som er behandlingsansvarlig.

[77] Jf. Ot. prp. nr 92 (1998-99) side 102.
[78] Jf. Ot. prp. nr 92 (1998-99) side 103
[79] Drøfting av behandlingsansvarlig i kapittel 2.5
[80] Jf. liste over enkeltvedtak ovenfor kommuner foretatt av Datatilsynet i 2008 og 2009
[81] Jf. Datatilsynet sak 09/00180 11. mai 2009 – Vedtak om pålegg – endelig kontrollrapport og dokument nr 3 – Endelig kontrollrapport – Notodden kommune punkt 5.1.
[82] Jf. Datatilsynet sak 08/00418 21. august 2008 – Vedtak om pålegg – endelig kontrollrapport – punkt 7.1 i endelig kontrollrapport.
[83] Jf. Datatilsynet sak 08/00353 29. september 2008 – Vedtak om pålegg – endelig kontrollrapport – punkt 7.1 i endelig kontrollrapport.

Forarbeidene påpeker at en og samme behandling av personopplysninger kan i enkelt tilfeller ha flere behandlingsansvarlige[84]. Dette er en aktuell problemstilling for kommuner, fordi det er blitt mer og mer vanlig at flere kommuner og fylkeskommuner etablerer interkommunalt samarbeid innen IKT-området. Kommunene har mulighet for dette med hjemmel i kommuneloven § 27. Lov om interkommunale selskap muliggjør også andre samarbeidsformer og gir noen føringer for denne typen virksomheter. Ved et interkommunalt samarbeid som omfatter informasjonssystemer, som behandler personopplysninger, vil kommunene kunne ha et delt behandlingsansvar. Pol gir ingen beskrivelse av dette forholdet. Schartum og Bygrave 2006 drøfter dette med delt behandlingsansvar og innfører også begrepet egentlig delt behandlingsansvar.[85] Dersom et interkommunalt samarbeid innebærer et forpliktende samarbeid der bestemmelsesretten over formål med behandlinger av personopplysninger og hvilke hjelpemidler som skal benyttes bestemmes i fellesskap, og der de enkelte kommunene er rettslig forpliktet til å følge det som blir bestemt, medfører dette egentlig delt behandlingsansvar.[86]

Som ovenfor nevnt kaller jeg databehandler for en aktør. Forarbeidene påpeker at begrepet databehandler er videre enn begrepet databehandlingsforetak slik det ble benyttet i personregisterloven[87] og databehandler omfatter også passive former for behandling, etter ønske fra en behandlingsansvarlig. Til denne aktøren gis det også i flere av de etterfølgende paragrafene oppgaver og fullmakter som gjelder sikring av personopplysninger. En databehandler skal også sørge for tilfredsstillende informasjonssikkerhet med hensyn på konfidensialitet, integritet og tilgjengelighet jf. pol § 13 første ledd. En databehandler skal på samme måte som en behandlingsansvarlig dokumentere informasjonssystemet og sikkerhetstiltakene jf. pol § 13 annet ledd. Forholdet mellom disse to aktørene, behandlingsansvarlig og databehandler, er også veldig interessant. Forholdet mellom disse gis i pol § 15 første ledd:

[84] Jf. Ot. prp. nr. 92 (1998-99) side 103.
[85] Schartum og Bygrave 2006 kapittel 2.5.1 til 2.5.5.
[86] Schartum og Bygrave 2006 kapittel 2.5.5 side 32.
[87] Lov om personregistre (opphevet)

En databehandler kan ikke behandle personopplysninger på annen måte enn det som er skriftlig avtalt med den behandlingsansvarlige. Opplysningene kan heller ikke uten slik avtale overlates til noen andre for lagring eller bearbeidelse.

En databehandler kan derfor ikke gjøre hva den vil med personopplysninger som den behandler på vegne av en behandlingsansvarlig. Databehandleren kan kun behandle personopplysninger på den måten som er skriftlig avtalt. I avtalen skal det også presiseres at databehandleren plikter å gjennomføre sikringstiltak som følger av pol § 13. Datatilsynet påpeker også viktigheten av databehandleravtale etter pol § 15. I vedtak ovenfor Stange kommune skriver de i sitt vedtak: [88]
Stange kommune må utarbeide databehandleravtaler med Hedmarken IKT og AS EDB i samsvar med personopplysningslovens § 15. Det vises til rapportens punkt 5.1.3. I tilsynsrapporten, som er vedlagt vedtaket, punkt 5.1.3 står det:
Personopplysningslovens § 15 stiller krav om at eventuelle databehandleres rådighet over personopplysninger på vegne av en virksomhet skal nedfelles i avtaleform. Kommunen benytter blant annet AS EDB for "hosting" av saksbehandlingssystemet Arkiv2000 og sikkerhetskopiering. Forholdet mellom partene er regulert i en forretningsmessig avtale, men har ingen elementer i forhold til personopplysningslovens krav Kommunen benytter Hedmarken IKT for drift av løsningen rundt publisering av postlister. Heller ikke mellom disse partene kunne det fremvises en databehandleravtale. Manglende databehandleravtale anses som brudd på personopplysningslovens § 15. Liknende presiseringer i vedtak og tilsynsrapporter finnes også i andre av Datatilsynets vedtak.[89]

Pol § 18 første ledd bokstav b og § 32 første ledd bokstav c beskriver "*hvem som har det daglige ansvaret for å oppfylle den behandlingsansvarliges plikter*". Her beskrives en rolle som kan kalles "den som har det daglige ansvaret". Forarbeidene beskriver denne samme rollen i forbindelse med at ledelsen i en virksomhet må sørge for at loven etterleves.[90] Som et ledd i dette kan de foreta en intern arbeidsfordeling, slik at det er klart hvilken stilling det ligger til å sørge for at loven etterleves i praksis. Det presiseres

[88] Jf. Datatilsynet vedtak 08/00254 punkt 3.
[89] Jf. Datatilsynet vedtak 08/00231, 08/00238, 08/00308.
[90] Jf. Ot. prp. nr 92 (1998-99) side 102.

videre at rollen bør knyttes til en lederstilling, slik at stillingsinnehaveren har reell daglig innflytelse på behandlingene som foretas. For en kommune vil det kanskje ofte være normalt at det er administrasjonssjefen[91], eller ofte kalt rådmann, som gis dette ansvaret. Det følger dessuten av kommuneloven § 23 nr 2 at administrasjonssjefen " skal sørge for at administrasjonen drives i samsvar med lover, forskrifter …". Det slås fast at det er rådmannen som har ansvaret for at kommunen er i samsvar med lover og forskrifter men for å kunne gjøre det på en tilfresstillende måte, er nok rådmannen avhengig av å delegere oppgaver innen behandling av personopplysninger og informasjonssikkerhet til underlagt personell. Det er normalt disse som har størst forutsetning for å vite hvilke tiltak som best sørger for etterlevelse av lover og forskrifter. Dette har han anledning til å gjøre, som en følge av kommunens interne organisasjons- og instruksjonsmyndighet. Delegering av personell kompetanse i et hierarkisk organ er som hovedregel tillatt.[92] Ved en melding til Datatilsynet etter pol §§ 31, 32 vil det derfor kanskje være anført at det er kommunen ved en eller annen sektordirektør eller enhetsleder som har det daglige ansvaret. Det bør derfor ikke alltid være rådmannen som blir anført til å ha det daglige ansvaret.

Pof § 2-3 første ledd lyder:

Den som har den daglige ledelsen av virksomheten som den behandlingsansvarlige driver, har ansvar for at bestemmelsene i dette kapittelet følges.

Her identifiseres en rolle som kalles "den som har den daglige ledelsen av virksomheten". Jeg vil ikke gå inn på en rettsdogmatisk drøftelse av hvem dette er men nøyer meg med å vise til kommunelovens § 9 nr 3 og § 23 nr 1. Ordføreren er kommunens rettslige representant og det er administrasjonssjefen (rådmannen) som er øverste leder for kommunens administrasjon. Det kan sikkert i enkelte tilfeller hevdes at ordførerne er den som har den daglige ledelsen av virksomheten men ofte tror jeg det forstås slik at det er rådmannen som kan kalles den som har den daglige ledelsen. Dette er sikkert også litt avhengig av størrelsen på en kommune. Forarbeidene til pol påpeker at der en behandlingsansvarlig er en juridisk person så vil ansvaret for å etterkomme

[91] Jf. kommuneloven § 22.
[92] Jf. Erik Boe Bind 2 kapittel 41.210.

sikkerhetskrav påhvile virksomhetens ledelse.[93] Jeg drøfter derfor ikke dette videre her men påpeker at det er den som har denne rollen som har ansvaret for at bestemmelsene i kapittel 2 etterleves jf. pol § 2-3 første ledd siste setning.

En rolle som ikke er direkte beskrevet men som fremkommer som et implisitt personelt krav, er en sikkerhetsrevisor i pof § 2-5 første ledd. Her står det at sikkerhetsrevisjon skal gjennomføres jevnlig uten at det står nærmere om hvem som skal gjøre dette. Forarbeidene nevner ikke sikkerhetsrevisjon og har kun kommentarer på at det bør lages rutiner for hvordan tiltak skal evalueres.[94] Siden det heller ikke er nevnt at dette bør utføres av eksterne, så må en anta at sikkerhetsrevisjon kan utføres av personer i egen organisasjon. Veilederen til pol sier i kommentarene til pol § 2-7 om organisering at arbeidsoppgavene til sikkerhetsleder normalt vil blant annet omfatte sikkerhetsrevisjoner.[95] Dette gir også en føring på at sikkerhetsrevisor er en rolle som hører til innenfor den behandlingsansvarliges organisasjon.

Rollen som medarbeider hos den behandlingsansvarlige nevnes eksplisitt i pof § 2-8 første ledd. Her beskrives det at medarbeidere bare skal bruke informasjonssystemet for å utføre pålagte oppgaver. I pof § 2-8 annet ledd står det videre at medarbeiderne skal ha nødvendig kunnskap for å bruke informasjonssystemet i samsvar med fastlagte rutiner. I paragrafens overskrift så brukes betegnelsen personell som er et synonym for medarbeider. Medarbeider nevnes dessuten også i pof § 2-9 der de pålegges taushetsplikt.

Lenger ut i forskriften, i pof § 7-12 beskrives enda en mulig rolle i informasjonssikkerhetsarbeidet. Dette er rollen som uavhengig personverneombud. Denne rollen er kun en frivillig ordning som skal godkjennes av Datatilsynet. Oppgaven til dette personverneombudet går ut på å kontrollere at den behandlingsansvarlige følger hele pol med forskrift. Dette innebærer også reglene som gjelder for organisering av informasjonssikkerhetsarbeidet. Det brukes betegnelsen uavhengig selv om at det forutsettes at personene er ansatt i virksomheten. Begrepet uavhengig antar jeg går ut på

[93] Ot. prp. nr. 92 (1998-99) side 115
[94] Jf. Ot. prp. nr 92 (1998-99) side 115 og NOU 1997:19 – kapittel 21, kommentarene til § 11 og § 12.
[95] Personopplysningslovens kommentarutgave side 351.

at den personen som innehar denne rollen, ikke skal ha noen utøvende oppgaver i forhold til behandling av personopplysninger. Selv om jeg antar det, er dette uklart og denne uklarheten er omtalt i Schartum og Bygrave 2006.[96] En hensikt ved eventuelt å opprette et slikt personverneombud, vil være at virksomheten er unntatt meldeplikt til Datatilsynet etter pol § 31. Veiledningen til forskriften beskriver, at meldingen da i stedet for å sendes til Datatilsynet, sendes til personverneombudet.[97] Siden dette personverneombudet skal kontrollere etterlevelse av blant annet krav til sikring av personopplysninger, vil en ha mulighet for å legge en lang rekke kontroll og evalueringsoppgaver til dette personverneombudet. En kan også tenke seg at rollen som sikkerhetsrevisor etter pof § 2-5 vil kunne bli utført av et personverneombud.

Videre så identifiserer pof i § 2-5 annet ledd to aktører som kalles kommunikasjonspartnere og leverandører. Det slås fast i § 2-5 annet ledd at en sikkerhetsrevisjon skal vurdere bruk av disse to aktørene. Kommunikasjonspartnere og leverandører er også referert til i § 2-15 tredje, fjerde og femte ledd. I § 2-15 tredje ledd så står det at leverandører som gjennomfører sikkerhetstiltak eller som bruker informasjonssystemet på annen måte på vegne av behandlingsansvarlig, skal tilfredsstille kravene i forskriften. Det gis ikke så mye veiledning på hva en kommunikasjonspartner er men veiledningen til pof til § 2-15 nevner kort at en kommunikasjonspartner kan eksempelvis være en databehandler.[98] Hvorfor det da ikke bare er brukt begrepet databehandler sies det ikke noe om. Jeg velger til tross for dette å liste opp kommunikasjonspartner som en aktør siden den er nevnt som en aktør i pof §§ 2-5 og 2-15.

Forvaltningsloven har som ovenfor nevnt krav til taushetsplikt for opplysninger ”om noens personlige forhold”, jf. forvaltningsloven § 13 første ledd. Jeg nevnte i avsnitt 2.2.1 at forvaltningsloven gjelder for kommuner. Krav til sikring av konfidensialitet for disse opplysningene gis i forvaltningsloven § 13 c annet ledd. Forvaltningsloven sier at det er forvaltningsorganet som skal sikre dette. Forvaltningsorganet er ikke nødvendigvis det

[96] Jf. Schartum og Bygrave 2006 kapittel 10.1
[97] Personopplysningslovens kommentarutgave side 369.
[98] Personopplysningslovens kommentarutgave side 356

samme som den behandlingsansvarlige etter pol § 2 nr 4. Behandlingsansvarlig er etter loven som tidligere nevnt den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes. Behandlingsansvarlig og forvaltningsorganet vil ved noen tilfeller derfor være det samme og ved de fleste tilfeller vil det nok ikke være den samme. Dersom behandlingsansvarlig er nedover i kommunens organisasjon vil det ikke være samme subjekt som omfattes av sikringskrav etter pol som pålegges krav til sikring etter forvaltningsloven. Til tross for det så velger jeg ikke å kalle forvaltningsorganet en selvstendig aktør, men vil huske på dette forholdet når jeg forholder meg til krav til sikring etter forvaltningsloven eller i medhold av loven.

Eforvaltningsforskriften som er gitt med hjemmel i forvaltningsloven. Jeg forkorter eForvaltningsforskriften til efvf videre i oppgaven. Efvf § 1 angir formål og anvendelsesområde:

(1) Forskriftens formål er å legge til rette for sikker og effektiv bruk av elektronisk kommunikasjon med og i forvaltningen. Den skal fremme forutsigbarhet og fleksibilitet og legge til rette for samordning av sikre og hensiktsmessige tekniske løsninger. Forskriften skal legge til rette for at enhver på en enkel måte kan utøve sine rettigheter og oppfylle sine plikter i forhold til det offentlige.

(2) Forskriften gjelder for elektronisk kommunikasjon med forvaltningen og for elektronisk saksbehandling og kommunikasjon i forvaltningen når ikke annet er bestemt i lov eller i medhold av lov.

(3) Denne forskrift gir ikke grunnlag for å gjøre unntak fra de alminnelige reglene om forsvarlig saksbehandling i forvaltningsloven.

Forskriften skal blant annet legge til rette for sikker og effektiv bruk av elektronisk kommunikasjon med og i forvaltningen og legge til rette for samordning av sikre og hensiktsmessige tekniske løsninger. En kan også merke seg at § 1 nr 2 sier at forskriften gjelder når ikke annet er bestemt i lov eller medhold av lov. Efvf viker derfor for særregler som fremgår av eller i medhold av annen lov.[99] Efvf nevner også flere steder forvaltningsorganet, jf efvf §§ 4,5, 8 og 13. Veilederen til efvf beskriver at en rekke av de forhold som forskriften adresserer, retter seg mot forvaltningsorganene og deres ansatte. Den sier videre at flere av bestemmelsene kunne tenkes å være gitt som instrukser og

[99] Jf. Veileder til eForvaltningsforskriften kapittel 2.

ikke i forskrift, men at dette ikke ville vært tilfredsstillende i forhold til kommunene.[100] Staten har ikke instruksjonsmyndighet ovenfor kommunene, og derfor er det nødvendig at reglene gis i forskrift, for at de også skal komme til anvendelse for kommunene. Efvf § 5 nr 1 nevner spesielt at det er forvaltningsorganet som er ansvarlig for at risiko for uberettiget innsyn i opplysninger som er underlagt taushetsplikt eller som er underlagt krav til sikring for personopplysninger. Her finnes en direkte kobling til sikringskrav for personopplysinger og ansvaret for dette ligger hos forvaltningsorganet. Jeg drøftet ovenfor forholdet mellom behandlingsansvarlig og et forvaltningsorgan.
Efvf § 5 nr 4 gir også en kobling til behandling av personopplysninger:

(4) Ved kryptering av melding til forvaltningen skal forvaltningsorganets krypteringsnøkkel eller krypteringsnøkkel til en nærmere angitt enhet ved forvaltningsorganet benyttes. Hvis forvaltningsorganet benytter ekstern databehandler i henhold til personopplysningsloven § 15, kan databehandlerens krypteringsnøkkel benyttes hvis det godtgjøres, eller er alminnelig kjent, at databehandleren opptrer på vegne av forvaltningsorganet.

I forhold til det jeg har beskrevet ovenfor med hensyn til databehandler og avtale mellom behandlingsansvarlig og databehandler er det helt klart at et slikt forhold som beskrives her i efvf § 5 nr 4 skal beskrives i avtalen mellom kommunen som behandlingsansvarlig og databehandleren. Efvf nevner også forvaltningsansatte, jf. efvf § 18 og innehaver av signaturfremstillingsdata, jf. efvf §§ 20 og 23. Innehaver av signaturfremstillingsdata er bare en type ansatte hos forvaltningsorganet som har fått tilgang til bruk av signaturfremstillingsdata. Begge disse begrepene er det samme som pof omtaler som medarbeidere jf. pof §§ 2-8 og 2-9. Jeg velger derfor ikke å definere en ny rolle men velger å anse det efvf kaller forvaltningsansatte og innehaver av signaturfremstillingsdata som det samme som pof kaller medarbeidere.

Annet regelverk slik som kommuneloven og lov om interkommunale selskaper kan ha innvirkning på forhold som ansvar og myndighet. De gir ingen direkte krav til organisering av informasjonssikkerhetsarbeidet, men de gir noen regler som har innvirkning på personelle og materielle krav.

[100] Jf. Veileder til eforvaltningsforskriften kapittel 2.

Jeg fant ingen dommer som hadde direkte innvirkning på min inndeling av rettsregler relatert til organisering av informasjonssikkerhetsarbeidet. Jeg så også på Personvernnemnda sine avgjørelser men fant ingen som hadde betydning for spørsmål rundt roller eller aktører relatert til informasjonssikkerhetsarbeidet.

2.4.2. Oversikt over aktører i arbeidet med informasjonssikkerhet

Nedenfor har jeg satt opp de identifiserte aktørene i en tabell. Den behandlingsansvarlige skal sørge for tilfredsstillende informasjonssikkerhet for de personopplysningene som den behandler. Databehandleren skal også sørge for tilfredsstillende informasjonssikkerhet. Leverandøren gis også plikt til å tilfredsstille krav til informasjonssikkerhet i kapittel 2 i pof. Kommunikasjonspartnere gis ingen plikter etter lov og forskrift men nevnes kun som en aktør som skal tas med i betraktning i sikkerhetsarbeidet hos den behandlingsansvarlige. En databehandler vil også måtte vurdere bruk av kommunikasjonspartnere og leverandører i sikkerhetsarbeidet sitt fordi det følger av pol § 15 annet ledd at: ” *I avtalen med den behandlingsansvarlige skal det også gå frem at databehandleren plikter å gjennomføre slike sikringstiltak som følger av § 13*.”. Dette gjelder dermed også krav som er gitt i pof, og dermed gjelder pof § 2-15 tredje ledd som stiller krav som berører bruk av leverandører.

Personelle krav - Aktør	**Referanse**
Behandlingsansvarlig	Personopplysningsloven § 2 nr 4. Personopplysningsloven § 13 første ledd Personopplysningsforskriften § 2-3, § 2-7.
Databehandler	Personopplysningsloven § 2 nr 5 Personopplysningsloven § 13 første ledd Personopplysningsloven § 15 første og annet ledd.
Kommunikasjonspartner	Personopplysningsforskriften § 2-5 annet ledd Personopplysningsforskriften § 2-15 fjerde og femte ledd
Leverandør	Personopplysningsforskriften § 2-5 annet ledd Personopplysningsforskriften § 2-15 tredje, fjerde og femte ledd.

Tabell 2 - Oversikt over personelle rettsregler - Aktører

2.4.3. Oversikt over roller i arbeidet med informasjonssikkerhet

Nedenfor er tabellen med oversikt over alle de identifiserte rollene i informasjonssikkerhetsarbeidet.

Personelle krav - Rolle	Referanse
hvem som har det daglige ansvaret for å oppfylle den behandlingsansvarliges plikter	Personopplysningsloven § 18 første ledd bokstav b og Personopplysningsloven § 32 første ledd bokstav c. Kommuneloven § 23 nr 2. Organets interne organisasjons- og instruksjonsmyndighet.
Den som har den daglige ledelsen (daglig leder)	Personopplysningsforskriften § 2-3 første ledd Personopplysningsforskriften § 2-7
Sikkerhetsrevisor	Personopplysningsforskriften § 2-5 første ledd
Medarbeidere	Personopplysningsforskriften § 2-8 første og annet ledd. Personopplysningsforskriften § 2-9.
Personverneombud	Personopplysningsforskriften § 7-12

Tabell 3 - Oversikt over personelle krav - Roller

2.4.4. Samlet vurdering

For oppgaven min vil alle de aktuelle aktører og roller, som er beskrevet her være aktuelle å ta med i vurderingen når jeg skal gjøre undersøkelser i kommunene. For at en kommune skal være i samsvar med de rettslige personelle kravene som beskrives her, må alle de relevante rollene som er obligatoriske etter regelverket, være tilordnet stillinger i kommunes organisasjon. Det kan være ulike måter å gjøre dette på og det finnes ingen fasit på hvordan en kommune kan overholde de rettslige kravene til organisering av informasjonssikkerhetsarbeidet. Det som kan synes viktigst her er at de rollene som er identifisert faktisk kan finnes igjen i en kommunes organisasjon, og de personene som innehar de stillingene som har fått ansvaret for å ivareta den behandlingsansvarliges plikter, er klar over at de har fått dette ansvaret.

Det vil også være viktig at dersom aktørene som er beskrevet ovenfor er involvert i en behandling av personopplysninger, så skal ansvar og plikter i forhold disse, være

ivaretatt. I noen tilfeller kan det være at en liten kommune gjøre en avtale om at en databehandler skal ivareta alle aspektene ved ivaretakelse av informasjonssikkerhetsarbeidet. Da vil være helt avgjørende at avtalen med databehandleren ivaretar alle krav og plikter som påhviler kommunen, og at kravet i pol § 15 tredje ledd blir ivaretatt.

2.5. Prosessuelle krav

Ved gjennomgangen av tabellene[101] jeg laget for de prosessuelle kravene var det mange krav. For å prøve å drøfte disse kravene systematisk er det flere måter å gjøre dette på. Jeg kan starte fra toppen av tabellene og gå gjennom regelverkene kronologisk paragraf for paragraf. Dette har jeg gjort når jeg kategoriserte rettsreglene og satte de inn i tabellene. Ved drøftingen synes jeg dette ikke nødvendigvis gir samme oversikten. Jeg har derfor valgt å ta med de viktigste prosessuelle kravene og dele de inn i typer og drøfte hver type i samme avsnitt. Disse er:

- Etablering av sikkerhetsorganisasjon og lage en sikkerhetsstrategi
- Risikovurdering
- Sikkerhetsrevisjon
- Avvikshåndtering

Dette kan virke forvirrende fordi jeg i min drøfting hopper litt i forhold til kronologisk rekkefølge for paragrafer i for eksempel pof. Jeg tar også med relevant drøfting av efvf innenfor de enkelte typer av prosessuell krav og ikke kronologisk gjennom efvf. Jeg har valgt dette fordi jeg håper dette gir større klarhet rundt de prosessuelle kravene, selv om jeg hopper i rekkefølgen for paragrafene i regelverkene.

2.5.1. Nærmere om prosessuelle krav

Prosessuelle regler beskriver hvordan oppgaver innen informasjonssikkerhetsarbeidet skal gjennomføres på. For å identifisere de prosessuelle reglene som gjelder for organisering av informasjonssikkerhetsarbeidet, vil jeg også i hovedsak se på krav i lov

[101] Vedlegg 1-4.

og forskrift. Flere av bestemmelsene i regelverkene beskriver til en viss grad hvordan oppgaver skal gjennomføres og hvordan organiseringen av informasjonssikkerhetsarbeidet skal være. Tabellene i vedlegg 1-4 identifiserer flere prosessuelle regler. Jeg vil ikke kommentere alle, men konsentrere meg om de jeg anser som viktigst og de som har mest betydning for organisering av informasjonssikkerhetsarbeidet.

2.5.2. Etablering av sikkerhetsorganisasjon og lage en sikkerhetsstrategi

Allerede i pol § 13 første ledd så beskrives et prosessuelt krav. Her slås det fast at tilfredsstillende informasjonssikkerhet oppnås *gjennom planlagte og systematiske tiltak.* Her gis det en overordnet oppskrift på hvordan tilfredsstillende informasjonssikkerhet skal oppnås. Forarbeidene sier også at eksempler på organisatoriske tiltak, kan være å etablere klare ansvars og myndighetsforhold i organisasjonen, sørge for kompetanse for eget personell og bare autorisere personell for tilgang til personopplysninger ved behov. Disse eksemplene fra forarbeidene er tatt med videre i pof, der pof § 2-7 første ledd sier at det skal etableres klare ansvars og myndighetsforhold og at disse skal dokumenteres jf. pof § 2-7 annet ledd. Overskriften til pof. § 2-7 er dessuten også organisering. En kan derfor slå fast at regelverkene pålegger at det skal finnes en form for sikkerhetsorganisasjon, der ansvar og myndighet innen informasjonssikkerhetsarbeidet er bestemt, og at dette skal dokumenteres jf. pof § 2-7. Hvordan denne sikkerhetsorganisasjonen skal se ut vil være avhengig av mange faktorer. Avveining av sammensetning og omfang vil være styrt av pol § 13 første ledd som pålegger at tiltak skal iverksettes for oppnå ”tilfredsstillende informasjonssikkerhet”. Dette har jeg beskrevet ovenfor i tidligere avsnitt. Pof § 2-1 annet ledd sier også som nevnt i tidligere avsnitt, at de planlagte og systematiske tiltakene som treffes i medhold av forskriften skal stå i forhold til sannsynligheten for og konsekvens av sikkerhetsbrudd. Her gis det også en kobling til gjennomføring av risikovurdering jf. pof § 2-4 som er omtalt nedenfor. Det er forskriftens krav i pof § 2-1 som er førende og rent praktisk vil omfanget av tiltakene være avhengig av størrelse på en kommune, antall behandlinger av personopplysninger etc. Hvordan en sikkerhetsorganisasjon vil se ut vil derfor være helt avhengig av om vi

snakker om en liten eller stor kommune. Grunnen til det er at en sikkerhetsorganisasjon i stor kommune vil være mer omfattende er at det vil være flere behandlinger i en stor kommune og at det vil være mange flere ansatte og en mye større organisasjon. I en liten kommune vil flere roller som er identifisert kunne være lagt til samme stilling. For at det skal være praktisk å sørge for å ivareta alle forhold rundt sikring av personopplysninger i de forskjellige delene i organisasjonen, vil mange oppgaver være delegert til flere personer i en stor kommune enn i en liten kommune. At det skal finnes en sikkerhetsorganisasjon, der det skal være klare ansvars- og myndighetsforhold, har jeg ovenfor slått fast. Det vil være et skjønnsspørsmål om den etablerte sikkerhetsorganisasjonen er tilfredsstillende etter pof § 13 og pof § 2-1. Veilederen til pof sier i sine kommentarer til pof § 2-7 at det er viktig at ansvar og myndighet relatert til drift av informasjonssystemene (driftsledelse) og for oppfølging av sikkerhetsarbeid (sikkerhetsledelse), er klarlagt.[102] Den sier videre at det disse funksjonene som den deler inn i henholdsvis ”utøvende” og ”kontrollerende” bør ideelt sett legges til forskjellige medarbeidere i virksomheten. Den sier også at for mindre virksomheter vil det likevel være nødvendig å legge begge funksjoner til en og samme person. Veilederen innfører rollen sikkerhetsleder og sier at arbeidsoppgaver for sikkerhetsleder vil normalt omfatte forberedelse av ledelsesgjennomganger, gjennomføring av sikkerhetsrevisjoner samt kontroll med risikovurdering og avviksbehandling. Jeg har også sett på hva Datatilsynet har lagt vekt på i sine vedtak, som omhandler informasjonssikkerhet ovenfor kommuner og fylkeskommuner. Min opplisting her av de rettslige krav er helt i tråd med det Datatilsynet også fokuserer på. I vedtak ovenfor Oppland Fylkeskommune heter det i vedtaket:[103]

Oppland Fylkeskommune må etablere og dokumentere informasjonssikkerhet i samsvar med personopplysningsloven § 13 jf. personopplysningsforskriften kap. 2. Dette innbærer at fylkeskommunene må:

a. Dokumentere sikkerhetsmål og sikkerhetsstrategi i samsvar med personopplysningsforskriften § 2-3. Det vises til tilsynsrapportens 5.1.1

[102] Personopplysningslovens kommentarutgave side 350-351.
[103] Datatilsynets vedtak 08/01458, 2. januar 2009

b. Dokumentere gjennomføring av risikovurderinger i henhold til personopplysningsforskriften § 2-4. Se rapportene pkt 5.1.2.
c. Dokumentere rutiner for sikkerhetsrevisjon i samsvar med personopplysningsforskriften § 2-5. Det vises til tilsynsrapportens 5.1.3.
d. Dokumentere rutiner for håndtering av avvik og/eller sikkerhetsbrudd jf. personopplysningsforskriften § 2-6. Det vises til tilsynsrapportens 5.1.4.
e. Dokumentere virksomhetens organisering av sikkerhetsarbeidet jf. personopplysningsforskriftens § 2-7. Se rapportens pkt. 5.1.5.

I andre vedtak refererer Datatilsynet også generelt til pol § 13 og til kapittel 2 i pof.[104]

Pof § 2-3 tredje ledd slår fast at valg og prioriteringer i sikkerhetsarbeidet skal beskrives i en sikkerhetsstrategi. Det er derfor helt klart at det skal foreligge en sikkerhetsstrategi i virksomheten. Pof § 2-7 annet ledd slår fast at ansvars- og myndighetsforhold skal dokumenteres. Det vil være naturlig at en slik dokumentasjon plasseres i kommunens sikkerhetsstrategi. Siden disse to kravene henger så tett sammen er de behandlet her i samme underkapittel.

Bruken av informasjonssystemer skal også jevnlig gjennomgås for å vurdere om blant annet sikkerhetsstrategien gir tilfredsstillende informasjonssikkerhet, jf. pof § 2-3 tredje ledd. Dette beskriver en aktivitet innen sikkerhetsorganisasjonen og som gir føring på hvordan tilfredsstillende informasjonssikkerhet skal oppnås. Dette er også noe som forarbeidene til pol nevner. Det må innføres rutiner for å evaluere sikkerhetstiltak og dette er noe som en sikkerhetsorganisasjon må sørge for er innført, og at det er noe som faktisk gjennomføres.

Efvf stiller også opp krav til sikkerhetsmål og sikkerhetsstrategi i § 13 som også pof § 2-3 gjør som jeg beskrev ovenfor. Efvf § 13 nr lyder:

Forvaltningsorgan som benytter elektronisk kommunikasjon skal ha beskrevet mål og strategi for informasjonssikkerhet i virksomheten (sikkerhetsmål og sikkerhetsstrategi). Sikkerhetsstrategien skal danne grunnlaget for forvaltningsorganets beslutninger om

[104] Jf. Datatilsynets vedtak 08/00251, 23. mai 2008, Datatilsynets vedtak 08/00238, 11. april 2008

innføring og bruk av sikkerhetstjenester og -produkter på en helhetlig, planlagt, systematisk og dokumentert måte. Sikkerhetsstrategien skal inkludere relevante krav som er fastsatt i annen lov, forskrift eller instruks.

Det også interessant å se på efvf § 13 nr 3 bokstav g:

prosedyrer for behandling av personopplysninger og taushetsbelagt informasjon, jf. § 5 og § 24, se også personopplysningsloven5 § 13 og personopplysningsforskriften kap. 2;
Veilederen til efvf sier at fordi forvaltningsorganene vanligvis også vil behandle personopplysninger, vil kravene etter efvf § 13 være delvis sammenfallende med kravene til sikkerhetsstrategi etter personopplysningsloven § 13 og personopplysningsforskriften kapittel 2.[105] Det er verd å merke seg efvf § 13 nr 1 siste setning. Denne kommenterer også veilederen og påpeker at sikkerhetsstrategien også skal "inkludere relevante krav som er fastsatt i annen lov, forskrift eller instruks". Sikkerhetsstrategien bør altså gi en samlet oversikt over kravene til informasjonssikkerhet innenfor det enkelte forvaltningsorganets område.[106] I noteapparatet i veilederen til efvf påpekes det at efvf § 13 nr 1 siste setning peker på nødvendigheten av å se krav til informasjonssikkerhet i sammenheng og gjennomføre vurderinger og tiltak for informasjonssikkerhet på en helhetlig måte.[107] Jeg skal ikke utdype dette videre her, fordi jeg konsentrer meg i denne oppgaven om rettslige krav til sikring av personopplysninger, men peker bare på at efvf § 13 er spesielt viktig for alle forvaltningsorganer i forbindelse med generelt arbeid med informasjonssikkerhet.

Det er i pol eller pof ikke tatt med noen bestemmelse som pålegger at sikkerhetstiltak skal være bygget på anerkjente metoder. Jeg beskriver kravet til risikovurdering nedenfor og det nevnes i forarbeidene at det ikke ble tatt med noen bestemmelse om dette. Hvordan tiltak skal utføres er jo nettopp i kjernen av det jeg kaller prosessuelle krav. Når det gjelder de prosessuelle kravene i eForvaltningsforskriften, er det interessant at det er kommet inn en bestemmelse i § 13 nr 2 at virksomhetens sikkerhetsstrategi skal være utarbeidet i henhold til anerkjente prinsipper for informasjonssikkerhet. Efvf § 13 nr 2 lyder:

[105] Veileder til eForvaltningsforskriften kapittel 3.3
[106] Veileder til eForvaltningsforskriften kapittel 3.3 annet avsnitt.
[107] Veileder til eForvaltningsforskriften kapittel 6 – note 87.

Sikkerhetsstrategien skal være utarbeidet i henhold til anerkjente prinsipper for informasjonssystemers sikkerhet.

Her er dette momentet faktisk kommet inn i en forskrift, som er gitt av samme departement som har gitt pof. Et slikt krav er ikke tatt med i pol eller pof. Når det er sagt, så sier forarbeidene til pol riktignok at selv om det ikke står at anerkjente metoder skal brukes, så er det ikke til hinder for at standarder brukes som målestokk for å vurdere informasjonssikkerhetstiltak. Veiledningen til pof kommer også inn på dette temaet. Her henvises det til at bestemmelsene i pol § 13 skal tjene som grunnlag for å harmonisere sikkerhetsnivået for behandling av personopplysninger som er hjemlet i annen lovgivning.[108] Det kommenteres videre at sikkerhetsstandarden BS-7799[109] er blitt brukt som en del av grunnlaget ved utarbeidelsen av forskriften. Det kommenteres videre at det vil være mulig å vise samsvar med sikkerhetsreglene i forskriften, ved å vise til at en er sertifisert etter sikkerhetsstandarden. Dette er en nyttig informasjon for en kommune. Veilederen til efvf viser til at NS 17799 er en viktig standard.[110] Som jeg har vært inne på tidligere, så vil det avgjørende for sikring av personopplysning være om tiltakene gir tilfredsstillende informasjonssikkerhet jf. pol § 13 første ledd, altså en skjønnsmessig vurdering og basert på den forholdsmessige vurderingen jf. pof § 2-1 annet ledd. Dersom en kommune har tatt utgangspunkt i en sikkerhetsstandard for å lage sin sikkerhetsstrategi, vil dette derfor sannsynligvis være i samsvar med rettslige krav.

2.5.3. Risikovurdering

Pof § 2-4 pålegger gjennomføring av risikovurdering og beskriver hvordan dette skal gjøres. Pof § 2-4 beskriver altså hvordan dette skal gjøres og er et prosessuelt krav. Pof § 2-4 første ledd sier at det skal føres en oversikt over hva slags personopplysninger som behandles. Den sier videre at virksomheten selv skal fastlegge kriterier for akseptabel risiko forbundet med behandlingen av personopplysninger jf. pof § 2-4 første ledd siste setning. Pof § 2-4 annet ledd sier at risikovurdering skal gjennomføres for å kartlegge sannsynligheten for og konsekvenser av sikkerhetsbrudd. Den pålegger også i pof § 2-4

[108] Personopplysningslovens kommentarutgave side 344-346.
[109] BS-7799-2:2005 er det samme som ISO 27001:2005, jf. http://emea.bsi-global.com/InformationSecurity/Overview/index.xalter
[110] Veileder til eForvaltningsforskriften kapittel 6 note 88.

annet ledd siste setning at ny risikovurdering skal gjennomføres ved endringer. Pof § 2-4 tredje ledd sier at resultatet etter risikovurderingen skal sammenlignes med de fastlagte kriterier for akseptabel risiko jf. pof § 2-4 første ledd. Den henviser også i pof § 2-4 tredje ledd siste setning til pof § 2-2 som sier at Datatilsynet kan gi pålegg om sikring av personopplysninger og herunder fastlegge kriterier for akseptabel risiko. Pof § 2-4 fjerde ledd sier til slutt at resultatet av risikovurderingen skal dokumenteres.
Pof § 2-4 første ledd som sier som sagt at det er virksomheten selv som skal fastlegge kriterier for akseptabel risiko i forhold til behandling av personopplysninger. Alternativt kan Datatilsynet gi pålegg om dette, jf. pof § 2-2. For å kunne gjøre dette er en kommune avhengig av en del personer i sentrale posisjoner, som har greie på risikofaktorer for de ulike systemene som behandler personopplysninger. Her ser vi at gjennomføringen av en risikovurdering har nær sammenheng med sikkerhetsorganisasjonen som er omtalt i avsnittet ovenfor.

Pof § 2-4 annet ledd sier at det skal gjennomføres ny risikovurdering dersom det er gjort endringer som har betydning for informasjonssikkerheten. Dette presiserer igjen viktigheten av de sentrale personene i organisasjonen, som har vært med på tidligere risikovurderinger og at resultatet av risikovurderingene har blitt dokumentert, jf. pof § 2-4 fjerde ledd. Pof § 2-3 tredje ledd henviser som ovenfor beskrevet til pof § 2-2 som gir Datatilsynet kompetanse til blant å fastlegge kriterier for akseptabel risiko forbundet med behandling av personopplysninger. Dette er derfor en faktor som må tas hensyn til når en kommune skal gjennomføre en risikovurdering. Dersom Datatilsynet har gitt pålegg om dette til en kommune, vil dette være gitt i form av et enkeltvedtak, ved f eks et tilsyn eller et konsesjonsvedtak, og kommunen vil være klar over dette forholdet. Datatilsynet vil dessuten kunne fatte et enkeltvedtak for et gitt saksbehandlingssystem for kommunesektoren. Dette vil de kunne gjøre siden det gjelder en bestemt krets av juridiske personer et slikt enkeltvedtak omfatter. Dersom det skal gjelde alle som behandler personopplysninger ville det måtte gjøres i form av en forskrift foretatt av Fornyings- og administrasjonsdepartementet (FAD), siden det er FAD som er delegert forskriftskompetansen.[111] Datatilsynet har gjort mange enkeltvedtak[112] der

[111] Forskrift av 11. april 2008 nr 345 (Deleg. til FAD etter personopplysningsloven)

risikovurdering nevnes. Risikovurdering er faktisk det som nevnes i nesten alle vedtak, der det er foretatt et tilsyn i 2008 og 2009, med hensyn på informasjonssikkerhet i kommuner. Eksempler på dette er gjengitt nedenfor. Vedtak ovenfor Ørskog Kommune:[113]

Kommunen må gjennom bruk av risikovurderinger etablere tilfredsstillende informasjonssikkerhet innen pleie- og omsorgstjenesten i samsvar med helseregisterlovens § 16, jf. personopplysningsforskriftens §§ 2-4 og 2-11. Det vises til tilsynsrapportens 5.2.3.

Samme ordlyd er brukt i vedtak ovenfor Orkdal kommune.[114]

Når forarbeidene kommer inn på systematiske tiltak nevner de risikoanalyse som en aktivitet som skal gjennomføres. Forarbeidene sier ikke så mye om hvordan en risikoanalyse skal utføres, annet enn at personopplysningenes antall og art skal vurderes opp mot trusler slik som f. eks i form av menneskelige feil, feil i programvare eller fysisk påvirkning. Dette er relativ lite veiledning når det gjelder risikoanalyse/risikovurdering. Veiledren til pof sier at en risikovurdering etter pof § 2-4 kan utføres med utgangspunkt i norsk standard NS-5848[115], Krav til risikoanalyser.[116] Selv om som ovenfor beskrevet pof § 2-4 gir føring på hvilke momenter som i hvert fall skal vurderes ved gjennomføring av en risikovurdering vil en finne mye veiledning i en sikkerhetsstandard for gjennomføring av risikoanalyse.

Efvf stiller også opp krav til vurdering av risiko. Efvf § 5 nr 1 lyder:

Når et forvaltningsorgan legger til rette for bruk av elektronisk kommunikasjon for mottak av opplysninger som på forvaltningens hånd kan være underlagt taushetsplikt, eller som kan være underlagt krav til sikring etter reglene om behandling av personopplysninger eller tilsvarende regler, skal risiko for uberettiget innsyn i opplysningene være forebygget på tilfredsstillende måte.

Her stilles det opp et krav at til dersom et forvaltningsorgan legger opp til mottak av opplysninger som er underlagt taushetsplikt eller underlagt sikringskrav etter regler for

[112] Jf. Datatilsynets vedtak 08/00231, 08/00238, 08/00252, 08/00306, 08/00307, 08/00308, 08/00309, 08/00310, 08/01458 med flere.
[113] Jf. Datatilsynets vedtak 08/00308 3. oktober 2008
[114] Jf. Datatilsynets vedtak 08/00309 15. august 2008
[115] Risikoanalyse – Veiledning til NS 5814
[116] Personopplysningslovens kommentarutgave side 349

behandling av personopplysninger, skal risiko for uberettiget innsyn i opplysninger være forebygget på tilfredsstillende måte. Her gis det derfor også et rettslig krav til gjennomføring av en risikovurdering. Risiko omtales også i efvf. § 5 nr 2 der forvaltingsorganet skal på hensiktsmessig måte informere om risiko nevnt i § 5 nr 1. I efvf § 8 nr 4 påleggs også forvaltningsorganet å forebygge risiko for uberettiget innsyn i enkeltvedtak. For å kunne gjøre dette må det nødvendigvis være gjennomført en risikovurdering.

Personvernnemnda behandlet i 2007 en klage på et vedtak gjort av Datatilsynet som blant annet omhandlet gjennomføring av risikovurdering.[117] Datatilsynet gjorde et vedtak som sa at en behandling av personopplysning ikke var tilstrekkelig i henhold pol § 13 og kapittel 2 i pof. Personvernnemnda var ikke enig med Datatilsynets vedtak og sa blant annet i sin vurdering.

Personvernnemnda viser til at Datatilsynet har en veiledningsplikt etter forvaltningsloven. Denne veiledningsplikt innebærer at tilsynet burde ha gitt Kolumbus en anvisning på hva en risikovurdering skal inneholde for å tilfredsstille personopplysningsforskriften kapittel 2. Det følger videre av personopplysningsloven § 13 og personopplysningsforskriften § 2-4 at det må foreligge en tilfredsstillende risikovurdering før løsningen kan vurderes. Tilsynet burde derfor også ha påpekt mangler ved den oversendte risikovurderingen, og gitt Kolumbus anledning til å rette opp disse, før tilsynet vurderte løsningen. I denne saken er dette ikke gjort.

Uansett avgjørelse i saken så viser dette at for å oppnå tilfresstillende informasjonssikkerhet etter pol § 13 må det gjennomføres en risikovurdering i henhold til pof § 2-4. Grunnet til at Personvernnemnda sendte denne saken tilbake til Datatilsynet var at de mente Datatilsynet ikke hadde gitt selskapet Kolumbus nok veiledning på hva en risikovurdering skal innholde for å tilfredsstille pof § 2-4, og dermed ikke hadde oppfylt sin veiledningsplikt etter forvaltningsloven.

2.5.4. Sikkerhetsrevisjon

Pof § 2-5 slår fast at det skal gjennomføres sikkerhetsrevisjoner. Dette krever derfor på samme måte som risikovurdering, at det er noen i virksomhetens organisasjon som har fått ansvaret for denne aktiviteten, og at dette utføres regelmessig. Dette kravet er også

[117] PVN-2007-04

knyttet til det personelle kravet, at det implisitt skal være en som har oppgaven å være sikkerhetsrevisor, se avsnitt 2.4.1. Grunnen til at jeg tar med dette kravet her er at en sikkerhetsrevisjon skal omfatte vurdering av blant annet organisering av informasjonssikkerheten, jf. pof § 2-5 annet ledd. Dette gir litt mer veiledning på hvordan en sikkerhetsrevisjon skal gjennomføres. Siden forskriften sier at en sikkerhetsrevisjon blant annet skal vurdere organisering av informasjonssikkerheten, er dette et krav som kan få stor betydning for informasjonssikkerhetsarbeidet. Pof § 2-5 tredje ledd sier at dersom en sikkerhetsrevisjon avdekker forhold som ikke er forutsatt, så skal dette behandles som avvik. Dette er dermed den tredje faktoren som pof gir oss når det gjelder hvordan en sikkerhetsrevisjon skal gjennomføres. Forarbeidene til pol sier at det bør lages rutiner for hvordan sikkerhetstiltak skal evalueres og dette kravet om sikkerhetsrevisjon i pof § 2-5 er således helt i tråd med forarbeidene. Veilederen til pof sier at sikkerhetsrevisjon er et viktig grunnlag for kontinuerlig forbedring av informasjonssikkerheten og rent praktisk så kan sikkerhetsrevisjoner gjennomføres etter de samme fremgangsmåter som benyttes i HMS-arbeid[118].[119]

Datatilsynet legger også vekt på sikkerhetsrevisjoner og utdrag fra vedtak ovenfor Oppland fylkeskommune er gjengitt nedenfor:[120]

Dokumentere rutiner for sikkerhetsrevisjon i samsvar med personopplysningsforskriften § 2-5. Det vises til tilsynsrapportens 5.1.3

I tilsynsrapportens 5.1.3 står det følgende:

I henhold til personopplysningsforskriftens § 2-5 skal det jevnlig gjennomføres sikkerhetsrevisjon av informasjonssystemet. Sikkerhetsrevisjon skal omfatte vurdering av organisering og om sikkerhetstiltak som er besluttet etablert faktisk er iverksatt og fungerer etter sin hensikt. Resultatet fra sikkerhetsrevisjonen skal dokumenteres. Oppland fylkeskommune opplyste under kontrollen at det ikke forelå klare rutiner for sikkerhetsrevisjon. Kravene i § 2-5 kan dermed ikke anses som oppfylt.

[118] Jf. internkontrollforskriften.
[119] Personopplysningslovens kommentarutgave side 350.
[120] Jf. Datatilsynets vedtak 08/01458.

I vedtak ovenfor Hordaland fylkeskommune står blant annet:[121]

Hordaland fylkeskommune må dokumentere tilfredsstillende informasjonssikkerhet jf. personopplysningslovens § 13 se rapportens pkt. 5.1. Dette innebærer at det må:

…

c. etableres et system for sikkerhetsrevisjon i samsvar med personopplysningsforskriftens § 2-5. Det vises til tilsynsrapportens pkt 5.1.3.

Videre i tilsynsrapporten gis en beskrivelse av hva Datatilsynet mener en sikkerhetsrevisjon innebærer, og gir samtidig veiledning på at en sikkerhetsrevisjon eksempelvis bør gjennomføres årlig:[122]

Virksomheten plikter i henhold til personopplysningsforskriftens § 2-5 å gjennomføre sikkerhetsrevisjon jevnlig, eksempelvis årlig. Sikkerhetsrevisjon skal omfatte vurdering av organisering og at sikkerhetstiltak som er besluttet etablert faktisk er iverksatt og fungerer etter sin hensikt.

Sikkerhetsrevisjon er et viktig grunnlag for kontinuerlig forbedring av informasjonssikkerhet i virksomheten. Resultatet fra sikkerhetsrevisjon vil være en del av grunnlaget for ledelsens gjennomgang jf. personopplysningsforskriftens § 2-3. Slik ledelsens gjennomgang vil ha som formål å vurdere hvorvidt de beslutninger som er tatt, er i samsvar med virksomhetens behov for informasjonsteknologi og informasjonssikkerhet.

Hordaland fylkeskommune kunne ikke dokumentere eller redegjøre for eksisterende rutiner for sikkerhetsrevisjon. Kravene kan dermed ikke anses som oppfylt.

2.5.5. Avvikshåndtering

Jeg nevnte i avsnittet ovenfor at dersom utfallet av en sikkerhetsrevisjon var uventet, så skulle dette bli behandlet som et avvik, jf. pof § 2-5 tredje ledd. Hvordan avvikshåndtering skal gjennomføres på reguleres i pof § 2-6 første ledd. Her sies det at bruk av et informasjonssystem som er i strid med fastlagte rutiner samt sikkerhetsbrudd, skal behandles som avvik. Pof § 2-5 annet ledd fortsetter å si at avviksbehandlingen skal

[121] Jf. Datatilsynets vedtak 08/01457 26. januar 2009. (hele vedtaket er ikke gjengitt men kun det som omhandler sikkerhetsrevisjon)
[122] Jf. Datatilsynets vedtak 08/01457, Endelig kontrollrapport punkt 5.1.3

ha som formål å gjenopprette normal tilstand. Det skal også fjerne årsaken til avviket. Som det siste momentet i denne paragrafen skal avvikshåndteringen også hindre gjentakelse av et avvik. Pof § 2-6 tredje ledd gir ytterligere føring på hvordan. Den sier at dersom avviket har medført uautorisert utlevering av personopplysninger, hvor konfidensialitet er nødvendig, så skal Datatilsynet varsles. Til slutt i pof § 2-6 fjerde ledd så skal avvikshåndtering dokumenteres. Dette er også en oppgave som skal gjøres men jeg har plassert det inn under et prosessuelt krav siden det at avviksbehandling skal dokumenteres, sier noe om hvordan en kan hindre gjentagelse av avvik, som pålegges som et prosessuelt krav i pof § 2-6 annet ledd. Som en sluttkommentar til avvikshåndtering så kan en si at dette også er en aktivitet som har en del å si for organiseringen av informasjonssikkerhetsarbeidet og utformingen av en sikkerhetsorganisasjon. Sikkerhetsorganisasjonen må sørge for at avvikshåndtering er ivaretatt og implementert alle steder, der det behandles personopplysninger i organisasjonen. Hvem som har ansvaret for dette, må derfor bestemmes og dokumenteres jf. avsnitt 2.5.2 om etablering av en sikkerhetsorganisasjon og sikkerhetsstrategi.

2.5.6. Samlet vurdering

I dette kapittelet har jeg behandlet prosessuelle rettsregler som jeg mener har mest betydning for organiseringen av informasjonssikkerhetsarbeidet. De prosessuelle rettsreglene jeg har tatt med er listet i tabellen nedenfor:

Prosessuelle krav	Beskrivelse	Referanse
Sikkerhetsorganisasjon	Et tiltak for hvordan tilfredsstillende informasjonssikkerhet skal oppnås. • Etablere klare ansvars og myndighetsforhold. • Disse forholdene skal dokumenteres. • Ansvars- og myndighetsforhold skal ikke endres uten autorisasjon fra kommunes daglige leder.	Pol § 13, pof § 2-7
Sikkerhetsstrategi	• Valg og prioriteringer i sikkerhetsarbeidet skal beskrives i en sikkerhetsstrategi. • Hvordan tiltak ivaretar informasjonssikkerheten skal beskrives. • Tiltak skal stå i forhold til sannsynligheten for og konsekvens av sikkerhetsbrudd.	Pol § 13, pof § 2-3 Efvf § 13
Risikovurdering	• Lage en oversikt over alle behandlinger av personopplysninger. • Fastlegge kriterier for akseptable risiko i forhold til behandling av personopplysninger. • Gjennomføre risikovurdering for å klarlegge sannsynligheten for og konsekvenser av sikkerhetsbrudd. • Gjennomføre risikovurdering etter endringer. • Risikovurderingen skal dokumenteres. • Resultatet av risikovurderingen skal sammenlignes med de fastlagte kriterier for akseptabel risiko.	Pof § 2-4 Efvf §§ 5 og 8

Sikkerhetsrevisjon	• Sikkerhetsrevisjon skal gjennomføres jevnlig. • Revisjonen skal omfatte vurdering av organisering, sikkerhetstiltak og bruk av kommunikasjonspartnere og leverandører. • Dersom revisjonen avdekker bruk som ikke er forutsatt skal dette behandles som avvik. • Sikkerhetsrevisjonen skal dokumenteres.	Pof § 2-5
Avvikshåntering	• Bruk av informasjonssystemer som er i strid med fastlagte rutiner skal behandles som avvik. • Sikkerhetsbrudd skal behandler som avvik. • Uforutsett bruk av informasjonssystemer som oppdages ved sikkerhetsrevisjon skal behandles som avvik. • Formålet med avvikshåndtering er å gjenopprette normal tilstand, fjerne årsaken til avviket og hindre gjentagelse. • Dersom et avvik har resultert i uautorisert utlevering av personopplysninger som trenger konfidensialitetsbeskyttelse, skal Datatilsynet varsles. • Resultatet av all avviksbehandling skal dokumenteres.	Pof §§ 2-5 og 2-6

Tabell 4 - Oversikt over de prosessuelle kravene

2.6. Samlet bilde av rettslige krav og betydningen for de videre undersøkelsene

Jeg har nå drøftet hvilken betydning de forskjellige personelle, materielle og prosessuelle kravene har å si for organiseringen av informasjonssikkerhetsarbeidet i en kommune. Jeg har endt opp med en liste over roller og aktører som identifiserer personelle krav. Jeg har også kommet fram til en liste over utvalgte prosessuelle krav, som jeg har identifisert som de viktigste for organiseringen av informasjonssikkerhetsarbeidet. Det er summen av disse kravene som jeg har kommet fram til, som jeg kaller de rettslige kravene til organisering av informasjonssikkerhetsarbeidet i kommuner. Jeg vil derfor i mitt videre arbeid i oppgaven, bruke disse kravene som referanse for mine undersøkelser. Når jeg skal kartlegge hvordan den faktiske organiseringen av informasjonssikkerhetsarbeidet er i de utvalgte kommunene i kapittel 3, vil jeg lete etter de identifiserte rollene og aktørene. Jeg vil under intervjuene spørre om aktører og roller og lete i dokumentasjon som jeg måtte få som sier noe om dette. Jeg vil også spørre om de aktivitetene som jeg har identifisert som prosessuelle krav. Her vil jeg spør om hvordan disse aktivitetene er utført, og samtidige se i dokumentasjon som beskriver hvordan disse aktivitetene skal gjennomføres.

3. Kartlegging av kommuners organisering av informasjonssikkerhetsarbeidet

3.1. Oversikt over fremstillingen i kapittel 3

Dette kapittelet handler om kartleggingen av faktisk organisering av informasjonssikkerhetsarbeidet i kommunene. Det jeg ønsker å få vite noe om er beskrevet i problemstilling nr 2 i oppgaven min:

> Hvordan har kommuner organisert informasjonssikkerhetsarbeidet?
>
> a) Hvordan er informasjonssikkerhetsarbeidet faktisk organisert?
> b) Hva har reelt sett vært styrende for organiseringen av informasjonssikkerhetsarbeidet? (regelverk, instrukser, avtaler, modeller, standarder mv)

Grunnlaget for hva jeg skal lete etter i min datainnsamling er som tidligere nevnt, kategoriseringen av rettsreglene i personelle og prosessuelle rettsregler. Denne kategoriseringen bidrar til å avgrense oppgaven slik at jeg spesielt leter etter disse faktorene i mine undersøkelser. Det vil samtidig være lettere å kategorisere resultatene etter datainnsamlingen og drøfte dette. Datainnsamlingen min, som sammenfattes i dette kapittelet, baserer seg på semistrukturerte intervjuer og dokumentanalyse av innsamlede instrukser og andre relevante dokumenter. Jeg ønsker å få belyst hvordan kommunen faktiske har organisert arbeidet, og da spesielt forholdene rundt roller og aktører innenfor personelle krav, og tiltak under prosessuelle krav. Jeg ønsker også å få belyst hva som reelt har vært styrende for organiseringen av informasjonssikkerhetsarbeidet.

3.2. Utarbeidelse av opplegget for datainnsamlingen

For å undersøke den faktiske organiseringen i kommunene, måtte jeg lage et praktisk opplegg for å gjennomføre datainnsamlingen. Som nevnt under metodedelen så har jeg valgt kvalitativ metode og da semistrukturerte intervjuer kombinert med dokumentanalyse av relevante dokumenter og instrukser. Intervjuene skulle gjennomføres

med nøkkelpersoner i kommunene som hadde spesiell kjennskap til informasjonssikkerhetsarbeidet.

Relevante informanter i kommunen for mitt opplegg vil være IT-sjef/sikkerhetssjef, administrasjonssjef/rådmann og eventuelt ordfører. På slutten av intervjuene vil jeg derfor spørre om relevante dokumenter og instrukser finnes.

En IT-sjef/sikkerhetssjef vil være den som vil ha mest detaljkunnskap om den faktiske organiseringen, og hvordan ting er gjort og litt om bakgrunnen for dette. Dette er fordi han er den som ofte har det daglige ansvaret for informasjonssikkerhetsarbeidet og har derfor mest detaljkunnskap. Jeg mener derfor at det vil være mest aktuelt å starte intervjuene med denne personen. Det er også det som problemstilling nr 2 a) er ute etter, den faktiske organiseringen. Når en beveger seg mot bakgrunnen for beslutninger, så går en over i problemstilling 2 b) og da vil det kunne være mer informasjon å hente ut og supplere med fra rådmenn. Bakgrunnen for hvorfor beslutninger er tatt og hvorfor ting er gjort på en bestemt måte, vil rådmannen ofte vite mer om, siden rådmannen normalt har ansvaret for å legge fram saker for kommunestyret. Til tross for det, antar jeg at dette vil være mest aktuelt i mindre kommuner. I større kommuner antar jeg at rådmannen har delegert mer saksforberedelse til IT-sjef eller sikkerhetssjef. Dersom kommunen har personvernombud vil det også være aktuelt å intervjue henne/han.

Rekkefølgen på eventuelle intervjuer av informanter i kommunen vil derfor være IT-sjef/sikkerhetssjef, eventuelt personvernombud og deretter ved behov rådmannen. Dersom jeg etter å ha gjennomført disse trenger mer informasjon, så vil jeg vurdere om det er nødvendig å intervjue rådmannen. Jeg vil bestrebe meg på å gjennomføre intervjuer med de samme stillingene i alle kommuner da det vil være lettere å analysere intervjuene i etterkant.

Når jeg skulle utforme spørsmålene, som også skulle være en hjelp for meg selv for å strukturere intervjuet, var det viktig å se på hva jeg hadde funnet under problemstilling 1. Her har jeg kartlagt hvilke rettslige krav som gjelder for organiseringen av arbeidet med å

sikre personopplysninger. Det er derfor viktig å bruke disse resultatene som bakgrunn for å kunne svare på spørsmålene under problemstilling 3, der jeg skal se på samsvar mellom faktisk organisering og rettslige krav. De 3 hovedkategoriene som jeg kategoriserte de rettslige kravene i kapittel 2 var personelle, materielle og prosessuelle krav.[123] Jeg endte opp med å avgrense slik at jeg kun så mer i detalj på kategori 1 – personelle krav og utvalgte krav under kategori 3 – prosessuelle krav.
Under personelle krav er det fokus på hvem som er tildelt myndighet eller oppgaver og endte jeg opp med to tabeller jf. Tabell 2 - Oversikt over personelle krav – Aktører, jf. Tabell 3 – Oversikt over personelle krav – Roller.
Under prosessuelle krav er det fokus på hvordan tiltak og oppgaver skal utføres og jeg endte opp med en liste over prosessuell krav, jf. Tabell 4 – Oversikt over prosessuelle krav.

I forkant av intervjuene planla jeg å gi en kort introduksjon til oppgaven min, og hvilke problemstillinger jeg hadde formulert. Det er viktig å presisere at dette skal være kvalitative intervjuer av typen semistrukturerte intervjuer. Jeg gikk derfor ikke slavisk gjennom spørsmålene, men hadde noen hovedspørsmål som utgangpunkt for samtalen med intervjuobjektene. Jeg hadde laget noen oppfølgingsspørsmål til hovedspørsmålene som jeg brukte ved behov under samtalen innen de tema som vi snakket om. Noen ganger fikk jeg bruk for oppfølgingsspørsmålene, men noen ganger gled samtalen naturlig over på disse og jeg trengte da ikke bruke disse. Det er viktig at intervjuene er fleksible og ikke låses fast i en definert ramme. Dette presiseres av Pål Repstad 2007.[124] Avhengig av svarene, kan samtalen endre kurs, og vi kan komme inn på tema eller problemstillinger, som ikke er omtalt i spørsmålene. Samtidig var jeg oppmerksom på at det var viktig at jeg under intervjuet ikke brukte for mye tid på urelevante områder. Det var derfor viktig å ha oppfølgingsspørsmålene, slik at jeg kunne styre samtalen inn på riktig spor, der vi kom litt ut av fokus. Etter at jeg hadde gjennomført et par intervjuer, vurderte jeg om jeg trengte flere oppfølgingsspørsmål. Jeg vurderte det slik at jeg kunne bruke de samme hoved- og oppfølgingsspørsmålene som jeg hadde brukt i de to første intervjuene. Ved

[123] Jf. Tabell 1 – Oversikt over kategorier av rettsregler som har betydning for organisering av informasjonssikkerhetsarbeidet
[124] Pål Repstad 2007 side 78-80

gjennomføringen av intervjuene spurte jeg om lov til å ta oppsamtalen på bånd, slik at jeg kunne gå gjennom intervjuet senere. Dette fikk jeg lov til og det var veldig nyttig ved gjennomgangen av resultatene. Jeg informerte også intervjueobjektene om at jeg kom til å anonymisere alle svarene. Jeg informerte om at verken navn på personer eller kommuner ville bli gjengitt i oppgaven min. Jeg tok i tillegg korte notater i stikkordsform under intervjuene. Etter hvert intervju gikk jeg rett i etterkant gjennom stikkordene og laget litt mer utfyllende notater. Når jeg kom hjem etter intervjuene hørte jeg gjennom lydopptakene og gjorde detaljerte notater. Jeg laget deretter en oppsummering av notater fra stikkordene og notatene fra lydopptakene, og sendte dette til intervjueobjektet for kommentarer. De fikk da rettet opp små feil og noen misforståelser. Jeg fikk også noen utfyllende kommentarer. I spørreskjemaet valgte jeg å dele inn hovedspørsmål på personelle krav og hovedspørsmål på prosessuelle krav. Jeg hadde også ett hovedspørsmål for hvilke faktorer som hadde vært styrende for organiseringen av informasjonssikkerhetsarbeidet. Hvert hovedspørsmål hadde flere oppfølgingsspørsmål. Hovedspørsmålene mine er:

Spørsmål	**Antall oppfølgingsspørsmål**	**Type rettslige krav**
Hvordan vil du beskrive organiseringen av arbeidet med informasjonssikkerhet i kommunen?	7	Personelle krav
Hva er etter ditt syn de viktigste utfordringene knyttet til organiseringen av sikkerhetsarbeidet?	3	Prosessuelle krav
Hvilke ting mener du er aller viktigst å huske på å ha med når det gjelder å organisere informasjonssikkerhetsarbeidet?	7	Prosessuelle krav
Hva har vært styrende for kommunens arbeid med hvordan organiseringen av informasjonssikkerhetsarbeidet er gjennomført på?	7	Hva som har vært styrende

Tabell 5 – Oversikt over hovedspørsmål og antall oppfølgingsspørsmål for gjennomføring av semistrukturert intervju

Det fullstendige spørreskjemaet ved gjennomføringen av de semistrukturerte intervjuene finnes i vedlegg 5.

3.3. Gjennomføringen av de semistrukturerte intervjuene

Da jeg hadde ferdigstilt opplegget for gjennomføringen av intervju, startet arbeidet med å ringe rundt til kommuner for å spørre om å få lov til å komme og gjennomføre et intervju. Siden jeg skulle gjennomføre kvalitative undersøkelser, og dermed ikke kan generalisere mine funn, så var det et poeng å prøve å finne kommuner som var forskjellige. Jeg ønsket å intervjue kommuner som var forskjellige i størrelse, og dersom noen hadde etablert et personvernombud, ville dette være interessant. Jeg viste også om flere kommuner som samarbeider om en IKT-leverandør. Det ville derfor være interessant å få til et intervju i en av disse kommunene. Måten jeg gikk frem på var at jeg fant ut hvem i kommunen som var sikkerhetsansvarlig eller IT-sjef, og ringte denne personen. Jeg presenterte meg og oppgaven min, og spurte om jeg kunne oversende mer info på e-post. Jeg spurte også om personen kunne tenke på om de ville stille opp til et intervju og gi meg beskjed. Jeg fikk deretter deres e-postadresse og sendt en e-post med litt mer informasjon om oppgaven, og hva jeg ville spør om. Det gikk ganske greit å få personer i kommunen til å stille opp til intervju. Jeg fikk nei kun av en kommune, og i en kommune var sikkerhetsansvarlig bortreist, slik at jeg måtte gå videre og spør en annen kommune. Jeg endte opp med å intervjue 4 kommuner som alle hadde noen ulike egenskaper. Jeg definerer i denne oppgaven små kommuner til å være kommuner med innbyggere med mindre enn 5000 innbyggere, en mellomstor kommune til å ha mellom 5000 og 20000 innbyggere og store kommuner som har innbyggere over 20000 innbyggere. I mine undersøkelser har jeg gjennomført 2 intervjuer i mellomstore kommuner og 2 intervjuer i store kommuner. Kommune B og D er store kommuner og kommune A og C er mellomstore kommuner. Valg av person som jeg skulle intervjue drøftet jeg i kapittel 3.2. Ved gjennomføringen av intervjuene fikk jeg ikke nok tid til å gjennomføre flere intervjuer i en kommune. På grunn av tiden jeg hadde til rådighet for datainnsamlingen måtte jeg nøye meg med å gjennomføre ett intervju i hver kommune. I kommune C hadde jeg avtale om 2 intervjuer, men dette ble avlyst på grunn av at IT-ansvarlig i kommunen måtte på tjenestereise. Dette medfører at informasjonen jeg fikk av intervjuobjektene kan

være ufullstendig. Jeg ville fått mer nøyaktig informasjon dersom jeg for eksempel hadde intervjuet alle personene som hadde definerte oppgaver innen sikkerhetsorganisasjonen. Dette kan også bety at noe informasjon kan være feilaktig. Dersom den jeg intervjuet for eksempel ikke visste om en risikovurdering var gjennomført, og dermed svarte nei på dette, ville dette bli en uriktig opplysning. Dette vil være en mulig feilkilde i mine innsamlede data. I kommune A intervjuet jeg IT-sjef. I kommune B intervjuet jeg IT-ansvarlig som også var sikkerhetsansvarlig. I kommune C intervjuet jeg personvernombud og i kommune D intervjuet jeg en IKT-rådgiver som var informasjonssikkerhetsansvarlig.

Under et par av intervjuene kom vi inn på flere av de prosesselle spørsmålene før vi kom inn på spørsmålene rundt personelle krav. Dette var ikke noe problem, da jeg på slutten av intervjuene så gjennom spørreskjemaet for å sjekke at jeg hadde vært innom alle hoved- og oppfølgingsspørsmålene. På den måten synes jeg spørreskjemaet fungerte veldig greit og etter sin hensikt. Jeg syntes selv at jeg klarte å la intervjuet flyte som en samtale, og ikke stykke det opp til å bli en samling av kun spørsmål og svar. På den måten fikk jeg også mer utfyllende informasjon rundt noen av problemstillingene, som jeg kanskje ellers ikke hadde fått tak i. Jeg fikk også etter intervjuene overlevert dokumentasjon som var relevant. Ved intervjuet i kommune A fikk jeg dokumenter tilsendt på e-post i etterkant av intervjuet. Etter intervju i kommune B ble relevant dokumentasjon omtalt, men jeg fikk dessverre ikke tilgang til dette. I kommune C fikk jeg relevant dokumentasjon overlevert under og rett etter intervjuet. I kommune D fikk jeg se gjennom relevant dokumentasjon rett i etterkant av intervjuet. Her fikk jeg notert meg viktig informasjon som jeg brukte i min videre analyse.

3.4. Kartlegging av praksis vedr personelle krav ved sikring av personopplysninger

3.4.1. Aktører og roller i Kommune A

I kommune A intervjuet jeg IT-sjef som også hadde oppgaver relatert til informasjonssikkerhetsarbeidet, og som derfor var en del av kommunens sikkerhetsorganisasjon. Etter intervjuet fikk jeg tilsendt diverse dokumenter og instrukser, og for kommune A var dette en rapport etter en forvaltningsrevisjon med hensyn på IKT-sikkerhet og sårbarhet, prosedyrer og dokumentert gjennomført risikoanalyse for IT-systemer, dokument som beskriver informasjonssikkerhet i kommunen (ikke formeldt vedtatt ennå) og en sikkerhetsinstruks for bruker av IT-systemene.

Ansvaret for alle behandlinger av personopplysninger ligger hos den behandlingsansvarlige. Dette er hovedaktøren/rollen innen de personelle kravene. Rollen som behandlingsansvarlig har kommunen et klart forhold til og kommunen er klar på at det er rådmannen som har dette overordnede ansvaret og er behandlingsansvarlig.

Kommunen bruker en databehandler til innsamling av personopplysninger i forbindelse med elektroniske søknader via Internett. Kommunens innbyggere kan søke på en rekke ulike tilbud via Internett. Ved innlevering av elektronisk søknad går disse først til et datafirma, som kommunen har en avtale med. Personopplysningene blir deretter overført til kommunens IT-systemer. Personopplysningene blir midlertidig lagret hos databehandleren og blir slettet etter en viss tid etter at kommunen har fått disse overført til sine egne IT-systemer. Kommunens avtale med denne databehandleren er gammel og utdatert, og er for øyeblikket under gjennomgang og revisjon, og vil bli fornyet i nærmeste framtid. Avtalen er veldig kort, og kommunen vet at den ikke inneholder det som kravene i regelverket sier. Dette er også grunnen til at kommunen reviderer avtalen, og planlegger å etablere en ny avtale i nærmeste framtid.

Kommunen har også en avtale med en innleid konsulent, når det gjelder IT-rådgivning. Denne personen har vært involvert med konstruksjon av systemløsninger, inkludert

tekniske sikkerhetsløsninger. Dette konsulentoppdraget faller derfor innenfor det jeg vil kalle bruk av leverandør.

Under intervjuet synes det klart at kommunen anser det som rådmannens oppgave å ivareta kommunens plikter som behandlingsansvarlig jf. pof § 2-3. Dette kommer også frem som følge av at kommunen har gjennomført en kommunerevisjon med hensyn på IKT-sikkerhet og sårbarhet. Denne revisjonsrapporten har vært forelagt kommunestyret og formannskapet, og det er rådmannen som er blitt gitt oppgaven med å gå gjennom denne og lage en tiltaksplan basert på funn i rapporten.
Informasjonssikkerhetsdokumentet presiserer også at det er rådmannen som har det overordnede ansvart for informasjonssikkerheten i kommunen.

Det er videre definert to andre konkrete personer som har det daglige ansvaret for å oppfylle den behandlingsansvarliges plikter jf. pol § 18. IT-sjef skal være ansvarlig for teknisk informasjonssikkerhet, og informasjonsleder skal være sikkerhetsansvarlig med et spesielt ansvar for rutiner og for sikker håndtering av personopplysninger. Det er videre planlagt at enhetsledere skal ha et ansvar for egen sektor, men dette er ikke formelt vedtatt ennå. Denne inndelingen av ansvar finnes ikke i forslaget til informasjonssikkerhetsdokumentet, men det er antydet i dokumentet at det skal være en person fra tre sektorer som skal ha oppgaver. Dette er en fra tjenestesektor, en fra skolesektor og en fra teknisk sektor. Fram til nå har det vært et løst definert ansvar hos enhetsledere for informasjonssikkerhet innen egne IT-systemer, men dette er ikke vært nedfelt i instruks av kommunens ledelse. Det er fokus på informasjonssikkerhet under IT-opplæring og ledermøter. IT-sjefen påpeker at det er en utfordring for kommunen å gi oppgaver innen informasjonssikkerhet til ansatte i kommunen, fordi den enkelte må utføre flere ulik oppgaver. Det er ikke økonomi til å ha egne stillinger til dette arbeidet. Han påpeker at det er den sikkerhetsansvarlige som har fått oppgaven med å kontrollere at sikkerhetsrutiner følges, men at det ikke er etablert rutiner for dette ennå. Det pekes på at aktiviteter som skal gjennomføres regelmessig må inn i det de kaller årshjulet, slik at aktivitetene innen informasjonssikkerhetsarbeidet blir tatt med i planleggingen av alle aktivitetene som skal gjennomføres hvert år.

Kommunen har fått gjennomført en revisjon foretatt av de som foretar normal internrevisjon i kommunen. Dette har satt i gang en mer generell revisjonsprosess i kommunen, som har vært styrt av sikkerhetsansvarlig i kommunen. Det fremgår av informasjonssikkerhetsdokumentet at det er sikkerhetsansvarlig som skal lede arbeidet med sikkerhetsrevisjon i kommunen. Rollen som sikkerhetsrevisor er derfor identifisert i dokumentasjonen, og faktisk tatt i bruk ved at sikkerhetsansvarlig har hatt oppgaver ved å revidere instrukser og prosedyrer.

Når det gjelder brukere av IT-systemene og deres rolle så har kommunen opplæringsprogram før de nyansatte gis tilgang til IT-systemene. Det fremgår at sikkerhetsinstruksen for bruker av IT-systemene, at den enkelte bruker skal ha lest gjennom og underskrevet. Det fremgår av instruksen at den enkelte ansatte har ansvar for at sikkerhetsrutinene følges. Den underskrevne originalen av dokumentet lagres hos personalkontoret i kommunen.

Kommunen har ikke implementert den frivillige ordningen med personverneombud jf. pof 7-12.

3.4.2. Aktører og roller i Kommune B

I kommune B intervjuet jeg IT-sjef, som også hadde rollen som sikkerhetsansvarlig. Han refererte til mange ulike instrukser, skjemaer og liknende og hva som var dokumentert. Jeg fikk dessverre ikke tilgang til disse, men fikk kun en muntlig beskrivelse.

Aktøren/rollen som behandlingsansvarlig, har kommunen et klart forhold til og kommunen her er også veldig klar på at det er rådmannen som har dette overordnede ansvaret.

Kommunen bruker ikke databehandlere for innsamling av personopplysninger, men utfører all innsamling selv. Kommunen opererer som databehandler for andre kommunale og interkommunale selskaper. Kommunen har derfor ikke databehandleravtaler der de selv er behandlingsansvarlig.

Kommunen bruker leverandører, og har da et standardskjema der disse må skrive under på beskyttelse og bruk av personopplysninger, samt taushetsplikt.

Kommunen anser det som klart at det som rådmannens oppgave å ivareta kommunens plikter som behandlingsansvarlig jf. pof § 2-3. Ved beskrivelse av kommunens sikkerhetsorganisasjon, er det klart at dette ansvaret ligger hos rådmannen. Dette ansvaret er delegert til IT-ansvarlig i kommunen som har fått rollen som sikkerhetssjef i kommunen.

Det er flere i kommunes organisasjon som har fått delegert daglig ansvar for å oppfylle den behandlingsansvarliges plikter jf. pol § 18. Som sagt så er IT-ansvarlig delegert ansvar og myndighet som sikkerhetssjef. IT-ansvarlig har i tillegg en person i egen enhet, som har fått delegert rolle som sikkerhetsansvarlig. Denne personen har blant annet fått oppgaven med å lede et sikkerhetsforum, som kommunen har etablert. I dette sikkerhetsforumet sitter det en representant fra hver av kommunens sektorer som er helse, skole osv. Disse fungerer som sikkerhetsansvarlige for egen sektor, og har et overordnet ansvar for egen sektors informasjonssikkerhetsarbeid. Den enkelte enhetsleder har også ansvar og myndighet delegert i forhold til informasjonssikkerhet. I tillegg har hvert system en systemeier og en fagansvarlig som har fått ansvar og myndighet. Ved noen tilfeller er enhetsleder og systemeier samme person. IT-avdelingen har i tillegg en egen sikkerhetsgruppe der sikkerhetssjef, sikkerhetsansvarlig samt to personer som har fått spesielle sikkerhetsoppgaver når det gjelder tekniske sikkerhetstiltak. Alle disse ansvars- og myndighetsforholdene er nedfelt i kommunes sikkerhetspolicydokument.

Rollen som sikkerhetsrevisor er fordelt på flere personer i kommunen. Det er systemeierne sammen med de sikkerhetsansvarlige for hver sektor, som ansvaret for at årlige sikkerhetsrevisjoner gjennomføres.

Brukerne i kommunen har også sin rolle ved at de er ansvarlige for å følge de ulike sikkerhetsrutinene, som kommunen har innført. Kommunen legger mye vekt på opplæring og bevisstgjøring av de ansatte, og har tidligere gjennomført quiz på

kommunens intranett, der spørsmål rundt informasjonssikkerhet har vært stilt og svarene har vært å finne i sikkerhetspolicyen og IT-reglementet. På denne måten har kommunen IT-avdeling drevet et meget aktivt arbeid for å heve sikkerhetsbevisstheten hos den enkelte ansatte. Samtidig er det den enkelte enhetsleder som er ansvarlig for tilstrekkelig opplæring av den enkelte ansatte.

Kommunen har ikke implementert den frivillige ordningen med personverneombud jf. pof 7-12.

3.4.3. Aktører og roller i Kommune C

I kommune C intervjuet jeg kommunens personvernombud. Denne var en del av kommunes sikkerhetsorganisasjon. Jeg fikk under intervjuet kopi av diverse dokumenter og instrukser som var relevante i forhold til datainnsamlingen. Av dokumentene jeg fikk, var dette IT plan for kommunen, oversikt over alle behandlinger av personopplysninger, skjema for registrering av risiko og sårbarhet, driftsrutiner, avvikshåndtering, sikkerhetsstrategi, sikkerhetsinstruks for sikkerhetsansvarlig, sikkerhetsinstruks for bruker, oversikt over sikkerhetsorganisasjonen, databehandleravtale. Jeg fikk også følgende godkjente instrukser: Instruks for bruk av Internett, Instruks for behandling av e-postkasser og private filer ved avsluttet arbeidsforhold, instruks for innsyn i e-post, instruks for bruk av e-post, rutiner ved ansettelse/opphør av arbeidsforhold, instruks for bruk av bærbart utstyr og instruks for bruk av hjemmekontorutstyr.

Kommunen var bevisst på at det var rådmannen som hadde hovedansvaret for alle behandlinger av personopplysninger. Kommunen var litt usikker på begrepet behandlingsansvarlig, og hadde valgt å kalle den som hadde ansvar for en bestemt behandling av personopplysninger som behandlingsansvarlig, jf kommunes oversikt over alle behandlinger av personopplysninger. Aktør som behandlingsansvarlig har derfor kommunen et forhold til, men litt uklar forståelse av begrepet. Det virket som det var en liten begrepsforvirring rundt begrepene behandlingsansvarlig jf. pol § 2 nr 4 og § 13 i forhold til hvem som har det daglige ansvaret for å oppfylle den behandlingsansvarliges plikter jf. pol § 18 og § 32.

Kommunen bruker også en databehandler til innsamling av personopplysninger i forbindelse med elektroniske søknader via Internett. Kommunens innbyggere kan søke på en rekke ulike tilbud via Internett. Selve søknadene går først til et datafirma, som kommunen har en avtale med. Ansvaret for etablering av avtalen ligger hos IT-sjef, men personvernombudet hadde også en kopi av denne. Jeg fikk derfor en kopi av denne. Personopplysningene blir deretter overført til kommunen IT-systemer. Databehandleravtalen inneholder krav som skal være ivaretatt jf. pol § 13 tredje ledd og pol § 15. Lagringen av personopplysninger hos databehandleren er kun midlertidig, og blir slettet etter en viss tid etter at kommunen har fått disse overført. Denne avtalen kom på plass etter at Datatilsynet hadde hatt tilsyn hos vedkommende databehandler, der det kom fram at personopplysninger ikke ble slettet.

Kommunen har også en avtale med et konsulentselskap, som er en leverandør og som har oppgaver relatert til støtte av en fagapplikasjon som behandler personopplysninger.

Kommunen var klar over ansvaret til kommunen som behandlingsansvarlig og at rådmannen hadde det daglige ansvaret for å overholde disse pliktene jf. personopplysningsforskriften § 2-3. Dokumentet som beskriver kommunes sikkerhetsorganisasjon bekrefter også dette. Videre så hadde kommunen definert flere personer som har det daglige ansvaret for å oppfylle den behandlingsansvarliges plikter jf. pol § 18. Kommunen hadde gitt en kommunelege rollen som sikkerhetsansvarlig. I tillegg hadde IT-ansvarlig og personvernombud ansvar og oppgaver. I tillegg til disse var også enhetsledere delegert oppgaver og ansvar for deler av informasjonssikkerhetsarbeidet.

Som følge av etablering av rollen som personvernombud, startet kommunen ledet av personvernombudet og IT-ansvarlig en revisjon av diverse instrukser. Den siste tiden har både personvernombudet og IT-ansvarlig hatt rollen som sikkerhetsrevisorer. Før etableringen av personvernombud, hadde kommunens sikkerhetsansvarlig gjennomført revisjon av rutiner og instrukser, og dermed fylt denne rollen tidligere.

Medarbeidere hadde også ansvar for ivaretakelse av informasjonssikkerheten, og det var laget en sikkerhetsinstruks for brukere av IT-systemene. Alle kommunens ansatte og konsulenter må skrive under på at de hadde lest sikkerhetsinstruksen for bruker, samt et skjema for taushetserklæring.

Dette var den eneste kommunen som hadde personvernombud. Dette er en frivillig ordning som kommunen ikke er pålagt å ha. Ordningen med personvernombud var kommet på plass som et resultat av at vedkommende hadde vært på kurs i regi av Datatilsynet. Her hadde Datatilsynet forespurt om kommunen var interessert i å opprette denne ordningen. Vedkommende hadde etter en tid, og etter en ny forespørsel fra Datatilsynet, tatt dette opp med rådmannen. Forslaget om å etablere dette ble deretter lagt fram for kommunestyret. Kommunestyret vedtok da at kommunen skulle gå inn i denne frivillige ordningen. Personvernombudet mente at det var to forhold som var viktige for et personvernombud. Disse var at vedkommende måtte ha god kjennskap til kommunens organisasjon, samt at en måtte være interessert i arbeidet med å sikre personopplysninger.

3.4.4. Aktører og roller i Kommune D

I kommune D intervjuet jeg en IKT-rådgiver i kommunen, som var kommunes informasjonssikkerhetsansvarlige. Denne personen hadde oppgaver relatert til informasjonssikkerhetsarbeidet. Rett i etterkant av intervjuet fikk jeg sitte ned å lese gjennom og notere fra håndboken i informasjonssikkerhet som de hadde fått laget.

Aktøren/rollen som behandlingsansvarlig har kommunen et klart forhold til, og kommunen her er også veldig klar på at det er rådmannen som har dette overordnede ansvaret.

Kommunen har et samarbeid med flere andre kommuner om felles drift av alle IT-systemer. Til dette er det etablert et interkommunalt selskap som eies av kommunene i fellesskap. Dette selskapet behandler personopplysninger på vegne av alle kommunene, og fungerer dermed som databehandler. Dette er et forhold som kommer inn under det

som en juridisk utredning kaller for egentlig delt behandlingsansvar.[125] Kommunen er klar over kravet til databehandleravtale men denne er ikke på plass ennå.

Kommunen forholder seg til leverandører når det gjelder IT-systemene, men avtalene med disse selskapene er mellom den enkelte leverandør og det interkommunale selskapet.

Kommunen beskriver rådmannen som den som har ansvar for å ivareta ansvar og plikter som behandlingsansvarlig jf. pof § 2-3. Dette går også frem av oversikten over kommunes sikkerhetsorganisasjon, i håndbok i informasjonssikkerhet. Her er rådmannen tegnet inn øverste i hierarkiet. Dette er også gjentatt under beskrivelsen av hvilke oppgaver den enkelte i kommunens sikkerhetsorganisasjon har.

Det er videre definert en person med helt konkrete oppgaver innen informasjonssikkerhetsarbeidet jf. pol § 18. IKT-rådgiver har fått delegert ansvaret som informasjonssikkerhetsansvarlig. Dette ansvaret er delegert fra rådmannen. Denne delegasjonen fremgår også av håndboken i informasjonssikkerhet. Kommunen sier videre at enhetslederne, systemeiere, systemansvarlige og brukere har roller i informasjonssikkerhetsorganisasjonen. Videre så peker håndboken i informasjonssikkerhet på at også styret i det interkommunale selskapet, den daglige lederen av selskapet, IT-sikkerhetsansvarlig og IKT-konsulenter har ulike roller.

Jeg får opplyst at det ikke er gjennomført noen systematiske sikkerhetsrevisjoner, men håndboken i informasjonssikkerhet sier at det er informasjonssikkerhetsansvarlig som skal gjennomføre årlige sikkerhetsrevisjoner. Rollen som sikkerhetsrevisor er derfor i dette tilfelle gitt til informasjonssikkerhetsansvarlig i kommunen.

Brukere er definert til å ha sin rolle i informasjonssikkerhetsarbeidet og de får også opplæring innen rutiner for informasjonssikkerhet før de får bruke systemene.

[125] Schartum og Bygrave 2006 side 32.

Kommunen har ikke implementert den frivillige ordningen med personverneombud jf. pof 7-12, men det har vært diskutert å etablere dette. Dette har også vært diskutert i et sikkerhetsforum som er etablert i det interkommunale samarbeidet. Det har også vært diskutert internt i kommunen.

3.4.5. Samlet vurdering

Alle kommunene hadde et klart forhold til aktøren og rollen som behandlingsansvarlig. Kommunene var samtidig klare på at det var rådmannen som hadde dette overordnede ansvaret.

De hadde også et klart forhold til aktøren databehandler. 3 av 4 kommuner brukte databehandler. Kravet om en databehandleravtale visste alle om, og hva denne i hovedsak skulle omfatte. Alle brukte det som regelverket kaller leverandør, men jeg fikk ikke identifisert andre aktører som kunne kalles kommunikasjonspartner. Etter at jeg hadde gjennomført mine undersøkelser i kommunene, publiserte Datatilsynet en ny veileder[126] som gir virksomheter mye hjelp til å opprette databehandleravtaler. Denne veilederen vil forhåpentligvis gjøre det lettere for kommuner å etablere gode databehandleravtaler.

I mine undersøkelser klarte jeg å identifisere alle rollene som jeg hadde kommet fram til under personelle krav. Riktignok hadde ikke alle kommunene alle rollene i sin organisasjon, men de fleste rollene var å finne i alle kommunene. For alle kommunene var rådmannen plassert i rollen som den som har den daglige ledelsen jf. pof § 2-3 første ledd

For rollene som faller under ”hvem som har det daglige ansvaret for å oppfylle den behandlingsansvarliges plikter” var det en del variasjon i kommunene. Her kom det mye an på kommunens størrelse. Jo større kommune var, jo flere personer identifiserte jeg som hadde fått delegert ansvar og myndighet innen informasjonssikkerhetsarbeidet.

[126] Datatilsynet – Databehandleravtaler etter personopplysningsloven og helseregisterloven - Veileder 26. mai 2009, http://www.datatilsynet.no/templates/Page____2747.aspx, sist besøkt 28. mai 2009

Rollen som sikkerhetsrevisor ble også identifisert i alle kommunene og i noen kommuner var det flere personer som hadde denne rollen.

I alle kommunene hadde dessuten medarbeiderne en klar definert rolle innen informasjonssikkerhetsarbeidet.

Rollen som personvernombud ble bare identifisert i en kommune. At jeg fikk vite at en kommune hadde denne ordningen, var en av grunnene til at denne kommunen ble valgt ut til intervju. I en av de andre kommunene hadde dette vært diskutert, men det var ikke tatt noen beslutning på om ordningen skulle etableres.

3.5. Kartlegging av praksis vedr prosessuelle krav ved sikring av personopplysninger

3.5.1. Prosessuelle tiltak i kommune A

Kommunens sikkerhetsorganisasjon beskrives av IT-sjefen. De identifiserte rollene som sikkerhetsansvarlig, IT-sjef med ansvar for tekniske sikkerhetstiltak, og enhetsledere hos den behandlingsansvarlige er beskrevet under personelle krav. Han beskriver også de ulike ansvars- og myndighetsforhold, som er gitt til de ulike stillingene innen kommunens sikkerhetsorganisasjon. Sikkerhetsorganisasjonen er også dokumentert i informasjonssikkerhetsdokumentet. Her er også ansvars- og myndighetsforhold beskrevet. Hvilket ansvar og myndighetsforhold som de ansvarlige for sektorene, tjeneste, skole og teknisk er ikke beskrevet. Dette har nok sin årsak i at dokumentet ikke er ferdigstilt ennå. Selv om dette ikke er beskrevet, så har dokumentet en lang liste som vedlegg, der alle kommunens behandlinger av personopplysninger listes opp. Her er den enkelte person eller stilling som har det daglige ansvaret for å oppfylle den behandlingsansvarliges plikter identifisert. Selv om at det beskrives i informasjonssikkerhetsdokumentet at det er kommunen ledelse som har det overordnede ansvaret, så bekreftes det under intervjuet at det er en utfordring å få ledernivået i kommunen til å ha fokus og bevissthet rundt problemstillingene, og krav i regelverk som kommunen må forholde seg til. Sikkerhetsorganisasjon omfatter også den enkelt ansattes

plikter, og det har kommunen implementert i forhold til at de har en sikkerhetsinstruks for brukere av IT-systemene.

I kommunens informasjonssikkerhetsdokument er det beskrevet en sikkerhetsstrategi med valg og prioriteringer samt sikkerhetsmål jf. pof § 2-3. Tiltak samt hvordan disse ivaretar informasjonssikkerheten er beskrevet.

Risikovurdering er også gjennomført i forbindelse med samarbeid med fylkesmannens beredskapskontor. Beredskapskontoret hos fylkesmannen har utarbeidet en mal for gjennomføring av risikoanalyse. Denne har kommunen brukt ved gjennomføringen av en risikoanalyse knyttet til tele- og ekomtjenester. Det bekreftes under intervjuet at det ikke er laget noen kriterier for akseptabel risiko, men noe ligger implisitt i slutten av rapporten etter risikoanalysen. I rapporten foreligger det forslag til prioriterte tiltak.

Som tidligere nevnt under analysen av personelle krav har det vært gjennomført en kommunerevisjon med hensyn på IKT-sikkerhet og sårbarhet, og det foreligger en revisjonsrapport. Målet for denne revisjonen var å undersøke etterlevelse av bestemmelsene i pol og pof. Sikkerhetsrevisjonen har omfattet sikkerhetsledelse, risikovurdering, sikkerhetsrevisjon, avvikshåndtering, organisering, personell og taushetsplikt, fysisk sikring, sikring av konfidensialitet, sikring av tilgjengelighet, sikring av integritet, sikkerhetstiltak, sikkerhet hos andre virksomheter og dokumentasjon. Jeg fikk opplyst at revisjonsrapporten er blitt forelagt kommunestyret og formannskapet, som har gitt rådmannen i oppdrag å lage en tiltaksplan, for å rette opp det som ble kommentert som mangelfullt i rapporten.

Når det gjelder håndtering av avvik så har kommunen ikke noe systematisk håndtering av disse. Rapporter om avvik blir håndtert når de kommer, men kommunen har ikke opplevd noen alvorlig hendelser. De har planer om å etablere et system for rapportering av avvik ved å bruke eksempelet til skjema fra veilederen til Datatilsynet som mal. Dette er ikke implementert ennå.

3.5.2. Prosessuelle tiltak i kommune B

De ulike rollene innen sikkerhetsarbeidet som utgjorde kommunens sikkerhetsorganisasjon ble beskrevet av IT-ansvarlig og er dokumentert under personelle krav. Rollen som sikkerhetssjef var delegert til IT-sjefen, som igjen hadde delegert ansvar for kommunens sikkerhetsforum til en sikkerhetsansvarlig. Den enkelte sikkerhetsansvarlig i hver sektor, hadde fått delegert sin oppgave fra sin sektordirektør. Ansvar for oppgaver til de ulike systemene var delegert fra sektordirektør til hver enkelt enhetsleder. Hver enhetsleder hadde enten ansvaret for å være systemeier selv, eller hadde delegert dette nedover i egen enhet. Samtidig hadde hvert system en fagansvarlig, som hadde det utøvende ansvaret for å ivareta sikkerhetsoppgavene. Alle oppgavene fremstår som klare og godt definert, og IT-sjefen sier at alt dette er godt dokumentert i sikkerhetspolicydokumentet. Sikkerhetsorganisasjon omfatter også den enkelt ansattes plikter, og det har kommunen implementert i forhold til opplæring og underskrift at de har lest og forstått sine plikter som bruker av informasjonssystemene.

Dette sikkerhetspolicydokumentet er kommunens sikkerhetsstrategi der ulike valg og prioriteringer er beskrevet jf. pof § 2-3. Denne policyen er godkjent av rådmannen. IT-reglementet er også en del av instruksverket rundt kommunens arbeid med informasjonssikkerhet.

Ved alle endringer, og ved innføring av nye systemer gjennomføres det risikovurderinger. Kommunen har utarbeidet egne skjema for dette. Det er de fagansvarlige for systemene sammen med sikkerhetsansvarlig for sektoren, som gjennomfører risikovurderingene. For IT-systemene er det IT-avdelingen som gjennomfører risikovurderingene. Alle risikovurderinger revideres årlig. IT-avdelingen er spesielt opptatt av risiko og er meget oppmerksom på risiko ved bruk av leverandører og ved kommunikasjon eksternt. Kommunen har erfart at eksterne leverandører, og spesielt statlige etater, har dårlig implementering av sikkerhetstiltak. Ved gjennomføring av risikovurderingene, er det systemeierne som er ansvarlig for å fastlegge kriterier for akseptabel risiko.

Kommunen gjennomfører også årlige revisjoner av informasjonssikkerheten. Til dette har de utviklet et skjema som samles inn av sikkerhetssjef. Organiseringen av arbeidet har

blitt vurdert tidligere, men kommunen har ikke gjort endringer i denne den siste tiden. Ved innføring av et større system gjennomførte også kommunerevisjon en revisjon, der sikkerhetspolicy og IT-reglement var grunnlaget for revisjonen. Kommunerevisjonen laget en rapport etter denne revisjon, som ble forelagt kommunens kontrollutvalg.

Kommunen har et eget system for avvikshåndtering. De har et utviklet et eget skjema for å registrere uønskede hendelser, som deretter behandles elektronisk. Systemet lager oversikter over avvik, og sørger for rapporter oppover i hierarkiet. Alle registrerte avvik tas også med i betraktning i revisjon av informasjonssikkerheten.

3.5.3. Prosessuelle tiltak i kommune C

Rollene som danner kommunes sikkerhetsorganisasjon er opplistet i avsnittet om personelle krav. Det finnes en sikkerhetsinstruks som beskriver ansvar og myndighet for sikkerhetsansvarlig. Kommunen har en sikkerhetsstrategi som er vedtatt i kommunestyret. Det fremgår av denne flere forhold rundt ansvar og myndighet, men det er ikke beskrevet alle oppgaver for IT-ansvarlig og personvernombud. Denne sikkerhetsstrategien er noen år gammel. I følge sikkerhetsinstruksen til den sikkerhetsansvarlige så har han hovedansvaret samt ansvar for at underlagte sikkerhetsledd har klart definerte oppgaver for å utøve sine funksjoner, og at de faktisk utøver disse. Personvernombudet mente at den sikkerhetsansvarlige ikke har nok tid til å arbeide med denne oppgaven. Flere av oppgavene som lå hos sikkerhetsansvarlig, ble utført av personvernombudet og IT-ansvarlig. Et konkret eksempel var utarbeidelse av diverse instrukser. På grunn av mangel på tid, hadde heller ikke personvernombudet fått sluttført disse. Dette forholdet hadde vært tatt opp til diskusjon med rådmannen. Enhetsledere hadde definerte oppgaver rundt behandlingen av personopplysninger. De hadde blant annet ansvaret for all opplæring av nytt personell samt sørge for avviksrapportering. De hadde også ansvaret for sine fagsystemer. IT-ansvarlig hadde ansvaret for implementering av alle sikkerhetstiltak relatert til IT-systemene. I forbindelse med godkjennelse av nye instrukser, hadde personvernombudet og IT-ansvarlig arrangert

informasjonsmøte med rådmannen og alle enhetsledere. På dette møtet ble alle instrukser gjennomgått og det ble informert om ansvaret alle enhetslederne har.

Som sagt ovenfor så hadde kommunen en sikkerhetsstrategi som var noe gammel. Personvernombudet ønsket å få til en revisjon av denne, men har dessverre litt for liten tid til å gjennomføre dette. Sikkerhetsstrategien gir en god overordnet beskrivelse av valg og prioriteringer, men er ikke veldig utfyllende på hvordan ulike tiltak ivaretar informasjonssikkerheten.

Det var noe uklart i hvilket omfang og hyppighet risikovurderinger utføres. Det bekreftes at det gjennomføres vurderinger i forbindelse med konkrete trusler. Kommunen hadde et skjema til dette men oppfattningen var at dette ikke var i utstrakt bruk. Å ha en oversikt over alle kommunens behandlinger av personopplysninger, er også en forutsetning for en god risikovurdering. Kommunens oversikt over dette var veldig bra og omfattende. Å ha denne oversikten er en del av personvernombudets jobb. Alle enhetsledere i kommunen sender oversikt over sine behandlinger til personvernombudet. Personvernombudet kunne ikke svare på hvem som eventuelt definerte kriterier for akseptabel risiko. Jeg fikk heller ikke overlevert dokumentasjon på om det var noen som hadde gjort dette. Kommunen opplyste at det ble gjennomført vurdering av risiko ved utplassering av IT-utstyr.

Kommunen hadde gjennomført revisjon av instrukser ved IT-ansvarlig og personvernombud. Flere av disse instruksene var nå godkjente i kommunens organer, men noen gjenstod. I forbindelse med at pol trådte i kraft 2001, gjennomførte kommunerevisjonen en revisjon med hensyn på krav i loven. Kommunerevisjonen er et interkommunalt samarbeid og tilsvarende revisjoner ble gjennomført i flere nabokommuner.

Kommunen hadde rutiner for avvikshåndtering, men instruksen var ikke ferdigstilt og vedtatt. Til tross for det så hadde det vært informert om innholdet i instruksen på et informasjonsmøte med alle enhetsledere. Etter dette møtet kom det etter hvert flere

avviksrapporter fra de ulike enhetsledere. Avvikshåndteringen til kommunen omfattet blant annet å finne årsaken til avviket. Dette for at sikkerhetstiltak kunne iverksettes, og dermed fjerne muligheten for at tilsvarende avvik skulle oppstå på nytt.

3.5.4. Prosessuelle tiltak i kommune D

Kommunens sikkerhetsorganisasjon beskrives av IKT-rådgiver. De mest fremtredende rollene som beskrives er rådmannen, informasjonssikkerhetsansvarlig og enhetslederne. Han beskriver også ansvars- og myndighetsforhold for de ulike rollene. Systemeiere og systemansvarlige er også personer som beskrives å ha en rolle for noen oppgaver innen informasjonssikkerhetsarbeidet, men beskrives ikke som noen som har en fremtredende rolle. Enhetslederne har ansvaret for all opplæring av egne ansatte, og for å gjøre sikkerhetsrutiner kjent i egen enhet og at de følges. Brukere har også oppgaver ved at disse må følge obligatorisk opplæring, samt at de har et selvstendig ansvar for å følge rutiner for informasjonssikkerhet. IKT-rådgiveren beskriver også et sikkerhetsforum som er etablert i regi av det interkommunale selskapet. I dette sikkerhetsforumet sitter informasjonssikkerhetsansvarlig fra alle kommunene, daglig leder og IT-sikkerhetsansvarlig i det interkommunale selskapet. Hele informasjonssikkerhetsorganisasjonen er veldig godt beskrevet i håndbok i informasjonssikkerhet som kommunen har. Her er også styret i det interkommunale selskapet inkludert i sikkerhetsorganisasjonen. Denne håndboken ble utarbeidet av et konsulentfirma i forbindelse med etableringen av det interkommunale selskapet. I håndboken er alle rollene, som er identifisert, nøye beskrevet med ansvar og oppgaver. I dette sikkerhetsforumet diskuteres blant annet sikkerhetsstrategien, sikkerhetstiltak og samarbeid om opplæring av ledere innen informasjonssikkerhet.

I denne håndboken er det også laget en felles sikkerhetsstrategi med beskrivelse av sikkerhetsmål jf. pof § 2-3. Håndboken inneholder dessuten mange skjema for diverse aktiviteter innen informasjonssikkerhetsarbeidet. Denne håndboken er svært omfattende og meget bra laget.

Kommunen gjennomfører risikovurderinger ved alle innføringer av nye systemer og applikasjoner. Det er informasjonssikkerhetsansvarlig sin oppgave å initiere disse risikovurderingene, men han trekker med enhetsledere/systemeiere og systemansvarlige i denne oppgaven. Det er som oftest systemeiere og systemansvarlige som faktisk gjennomfører risikovurderingen. I håndboken er det både skjema for gjennomføring av risikoanalyse og rapportskjema for risikovurderinger. Håndboken legger til rette for både litt enklere risikovurderinger og litt mer omfattende risikoanalyser. Kommunen er litt usikker på om det er definert kriterier for akseptabel risiko, men siden informasjonssikkerhetsansvarlig ikke er den som gjør dette selv, antar jeg at dette blir gjort av systemeierne.

Kommunen gir ikke uttrykk for at det er gjennomført noen sikkerhetsrevisjon, men i håndboken er det revisjonsguide for sikkerhetsrevisjon og skjema for rapport fra sikkerhetsrevisjon. Kommunen sier dessuten at i sikkerhetsforumet diskuteres sikkerhetsstrategi, organisering av sikkerhetsarbeidet og ulike sikkerhetstiltak. Jeg regner derfor med at mye av arbeidet som skal gjøres i forbindelse med en sikkerhetsrevisjon gjøres i regi av sikkerhetsforumet i det interkommunale samarbeidet.

For håndtering av avvik så har kommunen et eget fagsystem for avvikshåndtering. Dette dekker også kvalitetsrapportering. Kommunen har et økende antall faktisk rapporteringer. Det sier nok ikke så mye om at det er økende sikkerhetsbrudd men at de ansatte er flinkere til å rapportere avvik enn før. I forbindelse med at kommunen skal etablere en ny ansattportal, så ønsker informasjonssikkerhetsansvarlig via denne portalen å gjøre systemet med avviksrapportering ennå mer tilgjengelig. Alle rapporterte avvik lagres i en database. Avviksrapportene går til nærmete leder, som vurderer om avviket må rapporteres videre til rådmannen.

3.5.5. Samlet vurdering

Alle kommunene hadde en klart definert sikkerhetsorganisasjon. For det meste så var også ansvars- og myndighetsforhold beskrevet i dokumentasjonen. For de store

kommunene var sikkerhetsorganisasjonen større, og ansvar og oppgaver var fordelt på flere personer enn i de mellomstore kommunene.

Alle hadde dessuten også en sikkerhetsstrategi der valg og prioriteringer var beskrevet.

Risikovurderinger ble gjennomført i alle kommuner, men det var noe ulik praksis på hyppighet og hvem som gjennomførte disse. Alle risikovurderingene ble heller ikke foretatt på den måten som beskrives i pof § 2-4.

Hvem som hadde ansvaret for gjennomføring av sikkerhetsrevisjon var klart definert i kommunene, men det var ikke alle som kunne vise til en klar praksis på gjennomføring.

System for avvikshåndtering var systematisk implementert i 3 av de 4 kommunene og i den ene kommunen var dette behandlet noe mer på ad-hoc basis.

3.6. Kartlegging av hvilke faktorer som har vært styrende ved organisering av informasjonssikkerhetsarbeidet.

Under denne delen ville jeg prøve å få vite mer om hva som har vært styrende for kommunenes arbeid med organisering av informasjonssikkerhetsarbeidet. Dette vil si at jeg har sett etter faktorer som har vært med på å påvirke i større eller mindre grad kommunes arbeid. Her ville det vært spesielt interessant om jeg fant andre faktorer enn regelverkene, som hadde vært styrende. Jeg har i min problemstilling listet opp noen faktorer slik som regelverk, instrukser, avtaler, modeller og standarder som jeg har antatt har vært styrende.

Den viktigste faktoren som ble nevnt i alle kommunene som var årsak i kommunenes arbeid med å sikre personopplysninger var pol og pof. Hoveddelen av mine resultater fra intervjuene som relaterer seg til det jeg kaller personelle og prosessuelle krav er behandlet i kapittel 3.4 og 3.5. Disse ble drøftet i kapittel 2 og relaterer seg til kravene i pol, pof, forvaltningsloven og efvf. I dette kapittelet konsentrer jeg meg derfor om andre regelverk enn disse med et par unntak, samt andre styrende faktorer.

3.6.1. Faktorer som har vært styrende i Kommune A

Det første som ble nevnt under intervjuet her var veilederen som Datatilsynet har laget. Denne heter veiledning i informasjonssikkerhet for kommuner og fylker.[127] Denne veiledningen har sikkerhetsansvarlig i kommunen brukt som mal ved utarbeidelse av informasjonssikkerhetsdokumentet i kommunen. Her har de hentet ut mye av det som pol og pof stiller som krav, for at arbeidet med informasjonssikkerheten skal være tilfredsstillende.

Den andre kilden til veiledning som kommunen har brukt er revisjonsrapporten etter kommunerevisjonen, med hensyn på IKT-sikkerhet og sårbarhet. Formålet med denne

[127] Veiledning i informasjonssikkerhet for kommuner og fylker, Datatilsynet, TV-202:2005

forvaltningsrevisjonen har vært å undersøke i hvilken grad kommunens behandling av personopplysninger etterlever bestemmelsene i pol og personopplysningsforkskriften. Denne rapporten har derfor pekt på hva som er bra, og hva som ikke er ivaretatt i henhold til regelverket. Kommunen har derfor hentet mye veiledning fra denne rapporten, i forbindelse med informasjonssikkerhetsarbeidet.

Jeg spurte om de hadde brukt noen standarder eller liknende som veiledning med å organisere informasjonssikkerhetsarbeidet. De hadde ikke brukt dette, fordi han mente at sikkerhetsstandarder slik som fra ISO[128] var for omfattende i forhold til de resurser som kommunen hadde til å sette på et slikt arbeid. Standarder var derfor ikke et relevant sted å hente inspirasjon eller veiledning fra.

Kommunen var medlem av Foreningen for Kommunal Informasjonssikkerhet[129] (KINS) og mente at dette var en positiv aktivitet, som de anså å være en inspirasjonskilde for deres arbeid med informasjonssikkerhet.

3.6.2. Faktorer som har vært styrende i Kommune B

Kommunen hadde utviklet sin kompetanse på informasjonssikkerhet over tid. De nevnte ikke at de hadde hentet veiledning fra veilederen til Datatilsynet.

I forbindelse med utvikling av opplegg for gjennomføring av risikovurderinger, vurderte de et forslag til risikoanalyse som Direktoratet for samfunnssikkerhet og beredskap (DSB)[130] har utviklet. Dette mente kommunen ikke var veldig anvendelig for IT, siden dette opplegget opprinnelig var ment for alle sektorer. De hadde også sett på det Larvik kommune hadde gjort som var basert på en ISO standard. Kommunen mente at dette opplegget var veldig bra, men for omfattende. De falt derfor ned på en løsning for risikovurderinger som var enklere, og som de selv mente var gjennomførbart i praksis.

[128] International Organization for Standardization, http://www.iso.org/iso/home.htm , sist besøkt 5. august 2009
[129] Kommunal informasjonssikkerhet, http://www.kins.no/publisher/publisher.asp?id=1, sist besøkt 13. mai 2009
[130] Direktoratet for samfunnssikkerhet og beredskap (DSB), www.dsb.no siste besøkt 7. juni 2009

Det som både DSB og Larvik kommune har gjort, har derfor vært med på å veilede kommunen til å etablere et praktisk opplegg for gjennomføring av risikovurderinger.

De hadde tidligere hentet inspirasjon fra KINS, og var medlem her fra starten. Kommunen mener at det ikke lenger er så mye å hente av veiledning fra KINS, så de har derfor meldt seg ut. Til tross for det så deltar de ved behov på arrangementer i regi av KINS, dersom det er noe som er spesielt interessant for kommunen.

I tillegg deltok kommunens personell, som jobbet med tekniske sikkerhetstiltak, på ulike sikkerhetsfora der disse tekniske sikkerhetstiltak hadde fokus. Kommunen deltok på dette, fordi de så et behov for å inneha intern kompetanse når det gjaldt tekniske sikkerhetstiltak. Grunnen til dette var at de hadde erfaring med at samarbeidspartnere, ikke hadde tilstrekkelig kompetanse til å gjennomføre avtalte sikkerhetstiltak i praksis.

3.6.3. Faktorer som har vært styrende i Kommune C

Denne kommunen nevnte også Datatilsynets veileder som en av kildene, som kommunen har brukt mye, i forbindelse med informasjonssikkerhetsarbeidet. Kommunes personvernombud fikk dessuten den første versjonen av denne veilederen på høring, og kom med noen innspill før den ble ferdigstilt. Personvernombudet har også brukt juridisk litteratur knyttet til pol som støtte i forbindelse med informasjonssikkerhetsarbeidet.

Kommunen har som ovenfor nevnt etablert en frivillig ordning med personvernombud. Foranledningen til at dette ble etablert var at kommunes personvernombud var på opplæring hos Datatilsynet i forkant av etableringen av ordningen, og at personvernombudet var veldig interessert i arbeidet med å sikre personopplysninger. De aktivitetene som personvernombudet har vært med på i forkant av å bli utnevnt som personvernombud, og i etterkant, har også influert kommunens arbeid med informasjonssikkerhet. Det var rett i etterkant av etableringen av ordningen med personvernombud, at kommunen satte i gang en revisjonsprosess. Personvernombudet har dessuten blitt invitert til andre kommuner og til arrangementer i regi av KINS, for å

informere om rollen som personvernombud. Dette har hatt positiv innvirkning på kommunens arbeid med informasjonssikkerhet.

I forbindelse med at pol kom, gjennomførte kommunerevisjon en revisjon av informasjonssikkerhetsarbeidet. Dette påvirket også hvordan kommunen organiserte informasjonssikkerhetsarbeidet.

Kommunen deltar i et interkommunalt samarbeid der det er opprettet en arbeidsgruppe, som skal jobbe med spørsmål rundt informasjonssikkerhet. Dette er også en faktor som har påvirket kommunes arbeid med informasjonssikkerhet. Dette samarbeidet har også bidratt til å sette i gang ulike prosesser i de andre kommunene.

Kommunen er ikke medlem av KINS, men har planer om å melde seg inn. De har deltatt på arrangement i regi av KINS. Dette har også bidratt til å inspirere innen arbeidet med sikring av personopplysninger i kommunen. Personvernombudet uttrykte også ønske om en sterkere deltagelse fra Datatilsynet, der det eventuelt kunne vært arrangert møter mellom Datatilsynet og kommuner som hadde personvernombud, der også rådmannen var tilstede. Dette for å ha en jevnlig påminnelse til kommunens ledelse, om ansvaret for sikring av personopplysninger. Dette kunne hatt en positiv innvirkning til at kommunens ledelse ble sterkere involvert i arbeidet med organisering av informasjonssikkerhetsarbeidet.

3.6.4. Faktorer som har vært styrende i Kommune D

Kommunen nevnte at i forbindelse med etableringen av det interkommunale selskapet, ble det laget en håndbok i informasjonssikkerhet. Denne håndboken legger premissene for kommunens arbeid med informasjonssikkerhet, og på den måten styrer veldig mye hva kommunen skal arbeide med og hvordan kommunen arbeider. Håndboken henviser både til regelverkene men også til ISO 17799 og NS 5814. Dette viser at standarder har også vært en indirekte styrende faktor. Kommunen nevner at de også bruker veiledningsmateriell innen informasjonssikkerhet fra Datatilsynet.

Kommunen hadde ikke hatt noen spesielle revisjonsaktiviteter som hadde påvirket kommunens arbeid i vesentlig grad.

Kommunen har diskutert å etablere et personvernombud, men det er ikke etablert enda. Dette har derfor ikke vært med å påvirke arbeidet innen informasjonssikkerhet i kommunen.

Gjennom samarbeidet i det interkommunale selskapet, er det etablert et sikkerhetsforum. I forumet drøftes sikkerhetsstrategien, sikkerhetstiltak, opplæring etc. Dette samarbeidet er i stor grad styrende for kommunens organisering av informasjonssikkerhetsarbeidet. I regi av dette samarbeidet arrangeres det opplæring for ledere innen informasjonssikkerhet. I forumet er det også blitt drøftet etablering av en stilling som informasjonssikkerhetsansvarlig, som skal dekke alle kommunene i det interkommunale samarbeidet. Det er også drøftet om denne personen, dersom det etableres en ny stilling, også skal ha rollen som personvernombud for alle kommunene.

Kommunen er også medlem av KINS, og deltar her på konferanser og arrangementer, og henter mye inspirasjon til informasjonssikkerhetsarbeidet der.

3.6.5. Samlet vurdering

Under intervjuene i kommunene fant jeg flere samme faktorer i kommunene, som har virket styrende for organiseringen av informasjonssikkerhetsarbeidet. Kunnskapen om pol og pof er hovedårsaken til kommunenes arbeid med å sikre personopplysninger. Veiledninger fra Datatilsynet var også det som ble nevnt i tre kommuner. Enten selve veilederen eller veiledningsmateriell. Dette ble beskrevet å være en viktig faktor for et par av kommunene. For en av kommunene viste utarbeidelsen av en håndbok i informasjonssikkerhet seg som veldig viktig. Alle forhold rundt organisering og identifisering av personelle og prosessuelle krav var beskrevet i denne håndboken. Denne håndboken henviser dessuten til standarder for administrasjon av informasjonssikkerhet

og krav til risikovurderinger. Det viser seg også at revisjonsaktiviteter har vært en styrende faktor. Det var spesielt revisjon i regi av kommunerevisjonen, som har spilt en stor rolle. I en kommune var det etablert personvernombud. For denne kommunen har dette hatt stor betydning. Ulike interkommunale samarbeid ble også nevnt som en faktor, som påvirker informasjonssikkerhetsarbeidet i kommunene. For en kommune hadde også andre kommuners arbeid med risikoanalyser virket inn på arbeid med å lage egne rutiner. Et par typer sikkerhetsforum ble også identifisert som en styrende faktor. Medlemskap og deltagelse i KINS ble av alle kommunene nevnt som en faktor, som hadde spilt, eller for tiden spilte en rolle, for kommunes organisering av informasjonssikkerhetsarbeidet. Jeg vil i kapittel 4 komme nærmere inn på disse faktorene og drøfte betydningen disse har hatt for organiseringen av informasjonssikkerhetsarbeidet.

4. Forholdet mellom faktisk organisering og rettslige krav samt faktorer som har virket styrende på organiseringen

I dette kapittelet vil jeg drøfte resultatene mine, og prøve å gi svar på de innledende problemstillingene. I dette kapittelet var hensikten å prøve å svare på problemstilling 3 og 2b i oppgaven min. Problemstilling 3 lyder: Hvilket samsvar er det mellom hvordan organiseringen faktiske er gjennomført og de rettslige kravene?
Jeg har etter mine undersøkelser ikke nok datamateriale til kunne gjennomføre en ren rettsdogmatisk drøfting av samsvar. Når jeg skal drøfte samsvar vil jeg derfor se på om kommunene har et forhold til de roller og aktører som jeg identifiserte i den rettslige delen av oppgaven i kapittel 2. Jeg vil også se om jeg finner en sikkerhetsorganisasjon, om de har laget en sikkerhetsstrategi, om de gjennomfører risikovurderinger og sikkerhetsrevisjoner og om de har etablert avvikshåndtering. Jeg vil også kunne gi en antydning på om det jeg har funnet er i henhold til rettslige krav i regelverkene, uten at konkluderer om dette er i fullt ut i samsvar med rettslige krav. Jeg vil i denne drøftingen ikke ta for meg hver kommune enkeltvis, men se på alle kommunene i sammenheng.

Problemstilling nr 2 b lyder:
Hva har reelt sett vært styrende for organiseringen av informasjonssikkerhetsarbeidet? (regelverk, instrukser, avtaler, modeller, standarder mv)
Jeg synes at faktorer som har vært styrende for kommunenes organisering av informasjonssikkerhetsarbeidet er veldig interessant i et forvaltningsinformatisk perspektiv. Dette vil kunne være faktorer som ikke bare har rettslig karakter. Dette vil kunne være informatiske/teknologiske eller samfunnsvitenskapelige faktorer, som bidrar til bedre etterlevelse av rettslige krav.

Slike faktorer vil kunne være organisatoriske faktorer som viser seg i sikkerhetsorganisasjonen. Faktorer som et sikkerhetsforum og interkommunalt samarbeid vil være andre organisatoriske faktorer. Andre organisatoriske faktorer kan være størrelse på en kommune. Organisatoriske faktorer slik som interkommunalt samarbeid vil også kunne bidra positivt til sterkere samsvar med de rettslige kravene. Jeg har ikke kartlagt tekniske løsninger, men disse vil også kunne bidra til etterlevelse av rettslige krav. Disse faktorene vil derfor ikke ble belyst i denne oppgaven. Personellmessige faktorer vil være personer som er spesielt opptatt av å sikre personopplysninger som dermed får en spesiell rolle i etterlevelsen av krav. Et personvernombud er et eksempel på en slik faktor.

4.1. Samsvar mellom rettslige krav og faktisk organisering

4.1.1. Samsvar vedrørende personelle krav

Pol § 13 første ledd slår fast at det er den behandlingsansvarlige som skal sørge for tilfredsstillende informasjonssikkerhet. For å kunne etterleve dette kravet, må den som behandler personopplysninger være klar over at den er behandlingsansvarlig, og være klar over sitt ansvar etter loven. Undersøkelsene mine viser at alle kommunene er klar over dette, og at de er bevisst på lovens krav. Alle kommunene har dessuten iverksatt organisatoriske tiltak for å ivareta informasjonssikkerhetsarbeidet. Aktøren behandlingsansvarlig er identifisert og finnes i alle kommunene. Det virker derfor som alle kommunene har pekt ut behandlingsansvarlig i henhold til krav i regelverkene.

Pol § 13 tredje ledd pålegger den behandlingsansvarlige å påse at databehandlere som brukes, oppfyller de rettslige krav til informasjonssikkerhet. Dette skal gjøres gjennom en egen avtale med databehandleren jf. pol § 15 første ledd. Det minnes på i pol § 15 annet ledd at i denne avtalen skal det fremgå at databehandleren plikter å gjennomføre sikringstiltak, som følger av pol § 13. Alle unntatt en kommune bruker databehandlere. De er alle klar over at krav som følger av pol § 15 første ledd eksisterer. To av kommunene har etablert avtaler med databehandlere, mens en kommune ikke har dette på

plass. En kommune har dessuten en utdatert og gammel avtale. Aktøren databehandler finnes men ikke alle kommunene bruker dette. I forhold til bruk av databehandler er databehandleravtalen viktig rettslig krav. Det virker derfor som ikke alle kommunene tilfredsstiller de rettslige kravene til bruk av databehandler.

Pof § 2-5 stiller opp et krav om at bruken av leverandører og kommunikasjonspartnere skal være en del av en vurdering, som gjøres ved gjennomføring av en sikkerhetsrevisjon. Pof § 2-15 tredje ledd sier dessuten at leverandører skal tilfredsstille kravene i kapittel 2 i pof. Pof § 2-15 fjerde ledd pålegger den behandlingsansvarlige å påse at det etableres klare ansvars- og myndighetsforhold ovenfor leverandører og kommunikasjonspartnere. For å kunne gjøre dette, må det etableres en avtale mellom den behandlingsansvarlige og leverandøren. Flere av kommunene jeg har intervjuet bruker det som kalles leverandører. Der disse brukes er det etablert avtaler mellom kommunen og leverandøren. Jeg har ikke sett alle disse avtalene og dermed ikke kontrollert at de dekker det som de rettslige kravene pålegger. Det er derfor uvisst om kommunene opererer i samsvar med rettslige krav.

Pol § 18 første ledd bokstav b og pol § 32 første ledd bokstav c beskriver rollen, som jeg omtalt ovenfor, som den som har det daglige ansvaret for å oppfylle den behandlingsansvarliges plikter. Her stilles det ikke opp noe konkret krav til antall personer. Her er det helt opp den enkelte behandlingsansvarlige å utpeke personer i egen organisasjon, som skal ha dette daglige ansvaret. I undersøkelsene mine så identifiserte jeg mange personer i kommunenes organisasjon som falt inn under denne betegnelsen. De store kommunene hadde veldig mange personer som hadde oppgaver her, men også de mellomstore kommunene hadde veldig mange forskjellige personer, som var blitt gitt et slikt ansvar. Siden det ikke stilles et rettslig krav til antall som skal ha et slikt ansvar kan en ikke se på antall som har fått et slikt ansvar og deretter se på om det er i samsvar med rettslige krav. Hvor mange som har fått et slikt ansvar må nok holdes opp mot det jeg drøftet tidligere når det gjelder ”tilfredsstillende informasjonssikkerhet”, jf. pol § 13 og forholdsmessigheten jf. pof § 2-1. Siden jeg ikke har nok informasjon til å foreta en

vurdering om forholdsmessigheten er det uvisst om kommunene er helt i samsvar med rettslige krav.

Pof § 2-5 første ledd beskriver hvordan aktiviteten sikkerhetsrevisjon skal utføres. Rollen som sikkerhetsrevisor beskrives dermed implisitt. Det er ikke et rettslig krav til at det skal finnes en helt konkret stilling i organisasjonen som skal utføre dette. Det kan være forskjellige personer som utfører dette oppgaven. Alle kommunene har gitt denne oppgaven til en eller flere personer, og på den måten identifisert en rolle som sikkerhetsrevisor. Det vil helt klart være det beste at det er samme person som utfører dette regelmessig, fordi det kreves kunnskap om metoden for å kunne gjennomføre en sikkerhetsrevisjon. Jeg identifiserte denne rollen i alle kommunene og dette er en indikasjon på at det rettslige kravet til at en sikkerhetsrevisor skal finnes er ivaretatt.

Pof § 2-8 første og annet ledd samt pof § 2-9 nevner medarbeidere. Denne rollen er identifisert i regelverket, men den gir seg samtidig helt av seg selv. Dersom det finnes en behandlingsansvarlig med ansatte, vil det finnes medarbeidere. Innholdet i rollen utdypes i pof § 2-8 til at medarbeidere skal kun bruke informasjonssystemene til å utføre pålagte oppgaver, at de skal være autorisert for bruk og at de skal ha nødvendig kunnskap for å bruke informasjonssystemene i samsvar med de rutinene som er fastlagt. Dette gir medarbeiderne også et selvstendig ansvar for å bruke informasjonssystemene i samsvar med rutiner, men det pålegger også de som er ansvarlige for opplæring et ansvar. I alle kommunene er det fokus på dette med brukerinstruks for ansatte og opplæring. Dette er helt i tråd med det jeg identifiserte under de rettslige krav i kapittel 2. I flere av kommunene er det enhetslederne, som også har personalansvaret, som har ansvaret for at opplæring gjennomføres. Om alle kommunene følger alle kravene som regelverkene stiller til opplæring etc. til punkt og prikke er usikkert, da jeg ikke har nok detaljer til å svare på dette.

Rollen som personvernombud etter pof § 7-12 er kun en frivillig ordning. Det finne ikke noe rettslig krav til at denne rollen skal finnes i en kommunes organisasjon. Det er derfor ikke relevant å drøfte samsvar med regelverket for denne rollen men kun samsvar opp

mot krav til personvernombud dersom rollen finnes. Pliktene som hviler på personvernombudet er at den han/hun skal sikre at den behandlingsansvarlige følger pol med forskrift, og føre en oversikt over alle behandlingene av personopplysninger i kommunen. I kommunen der denne rollen er etablert, er det min oppfatning at personvernombudet helt klart er med på å sikre at kommunen følger pol med forskrift. Personvernombudet har dessuten også en omfattende oversikt over kommunenes behandling av personopplysninger. Det virker derfor at dette er i samsvar med de rettslige krav, men det jeg ikke si helt sikkert.

4.1.2. Samsvar vedrørende prosessuelle krav

Pol § 13 pålegger at det skal iverksettes planlagte og systematiske tiltak for å oppnå tilfredsstillende informasjonssikkerhet. § 13 fjerde ledd inneholder forskriftskompetansen for å kunne gi forskrift som gjelder informasjonssikkerhet. Det gis eksempler på hva dette kan være, og da nevnes organisatoriske og tekniske sikkerhetstiltak. Denne opplistingen er ikke uttømmende. Pof § 2-7 setter krav til at det skal finnes klare ansvars- og myndighetsforhold for bruk av informasjonssystemene, og at dette skal dokumenteres. I kombinasjon med de rettslige kravene til personelle krav er det disse to kravene som danner det rettslige grunnlaget for en sikkerhetsorganisasjon. Det er ikke gitt noe krav til antall personer som skal danne en sikkerhetsorganisasjon. Dette er nok det beste fordi dette regelverket omfatter alle som behandler personopplysninger, som helt eller delvis skjer med elektroniske hjelpemidler jf. pol § 3 første ledd bokstav a og pof § 2-1. Alle typer virksomheter er omfattet, og det vil derfor være vanskelig å pålegge et krav om antall personer til ulike sikkerhetsoppgaver. Alle kommunene hadde dokumentasjon med oversikt over egen sikkerhetsorganisasjon, samt dokumenterte ansvars- og myndighetsforhold. I den største kommunen var det mange personer som var en del av kommunens sikkerhetsorganisasjon, og i de mellomstore kommunene var det noen færre. Siden de rettslige kravene ikke pålegger en bestemt størrelse, så kan det virke som at dette er i samsvar med de rettslige krav. Til tross for det så må det også gjøres en vurdering på om det er tilfredsstillende i henhold til pol § 13 og står i forhold til sannsynlighet for og konsekvensen av sikkerhetsbrudd jf pof § 2-1. Dette har jeg ikke nok informasjon til å vurdere så det er derfor usikkert om kommunene tilfredsstiller de

rettslige krav til å etablere en sikkerhetsorganisasjon med klarer ansvars- og myndighetsforhold.

Pof § 2-3 stiller opp et konkret krav om at valg og prioriteringer i sikkerhetsarbeidet skal beskrives i en sikkerhetsstrategi. Overordnet så stiller også pol § 13 opp et krav til at sikkerhetstiltakene skal dokumenteres. Dette virker derfor sammen med pof § 2-3 om å etablere en sikkerhetsstrategi. Det gis litt veiledning på hvor en skal hente innspill til utforming av sikkerhetsstrategien. § 2-3 fjerde ledd og femte ledd stiller opp et krav om at bruk av informasjonssystemene skal gjennomgås jevnlig, og det skal deretter foretas en vurdering på om den eksisterende sikkerhetsstrategien gir tilfredsstillende informasjonssikkerhet. Alle kommunene hadde laget en sikkerhetsstrategi. Selv om en kommune ikke hadde ferdigstilt sikkerhetsstrategien, så kan en ikke påstå at den ikke finnes. To av kommunene hadde en veldig omfattende strategi mens de to andre hadde et mindre dokument. Det vil igjen være et skjønnsspørsmål om en slik sikkerhetsstrategi er omfattende nok. Det virker derfor på meg som at et par av kommunene er i samsvar med rettslige krav mens de to andre ikke er helt i samsvar.

Pof § 2-4 stiller opp et krav om at det skal gjennomføres en risikovurdering. Jeg var under den rettslige kategoriseringen inne på at det er flere krav som oppstilles til hvordan en risikovurdering skal gjennomføres på. En forutsetning for en risikovurdering, er at det finnes en oversikt over alle behandlingene av personopplysninger jf. pof § 2-4 første ledd første setning. En annen forutsetning som må være på plass, som vil være avgjørende, er at det må defineres kriterier for akseptabel risiko jf. pof § 2-4 første ledd annen setning. Det er disse kriteriene som skal brukes på slutten av risikovurderingen, når en skal vurdere om det skal iverksettes tiltak eller ikke, for å redusere identifiserte risikoer. Alle kommunene hadde sine oversikter over behandlinger på plass. Dette gir en god indikasjon på at kommunene har kontroll på hvilke personopplysninger de behandler. Dette gir en god indikasjon på samsvar med de rettslige kravene. En av kommunene svarte positivt på at det var systemeierne som definerte disse kriteriene for akseptabel risiko. De andre kommunene var mer uklare på dette punktet. Selv om to kommuner ikke kunne svar på om dette var definert, er det ikke helt utelukket at disse kriteriene var definert. Til tross

for det, så virker det for meg at på dette punktet, så er det ikke samsvar med de rettslige kravene. Det er også et krav om at det skal gjennomføres ny risikovurdering, dersom det gjøres endringer i informasjonssystemene som har betydning for informasjonssikkerheten. Det er kun en av kommunene som svarer helt konkret og bekreftende på dette punktet. De andre tre kommunene er litt usikre på hyppighet og om det faktisk skjer ved alle endringer. Selv om det angis at det gjennomføres risikovurderinger, så mangler det litt på at det er helt i samsvar med de rettslige kravene. Pof § 2-4 tredje ledd stiller opp et krav til at resultatet av en risikovurdering skal sammenlignes med de fastlagte kriteriene for akseptabel risiko. Siden flere av kommunene ikke kunne vise til disse definerte kriteriene, gir dette meg en sterk indikasjon på at dette ikke samsvarer med de rettslige kravene. Det stilles til slutt opp et krav til at selve risikovurderingen skal dokumenteres, jf. pof § 2-4 fjerde ledd. Her kan alle kommunene vise til dokumentasjon på at risikovurderinger er gjennomført. Totalt sett så har alle kommunene gjennomført risikovurderingen men det skorter litt på kvaliteten på gjennomføringene, og at de prosessuelle kravene er fulgt i henhold til regelverkene. Dette gir meg en sterk indikasjon på at gjennomføring av risikovurderinger i kommunene ikke er helt i samsvar med de rettslige kravene.

Pof § 2-5 første ledd pålegger at det jevnlig skal gjennomføres sikkerhetsrevisjoner. Pof § 2-5 annet ledd gir føringer på hva sikkerhetsrevisjonen skal omfatte. Det som listes opp er at den skal omfatte vurdering av organisering, sikkerhetstiltak og bruk av kommunikasjonspartner og leverandører. Alle kommunene har aktiviteter rundt sikkerhetsrevisjon. Det er flere ulike typer revisjoner. Dette omfatter revisjoner som er gjennomført av sikkerhetsansvarlig eller personvernombud, og revisjoner som er foretatt av kommunerevisjonen. Det stilles også opp et krav i pof § 2-5 fjerde ledd, at sikkerhetsrevisjonen skal dokumenteres. Hvordan dette skal gjøres er det ingen føringer på. De rettslige kravene sier ingenting om hvem som skal gjennomføre revisjon, man bare at den skal gjennomføres, og litt om hvordan. Jeg gikk ikke inn i detaljer rundt hvordan kommunene hadde gjennomført sine sikkerhetsrevisjoner. Alle kommunene har eller har hatt revisjonsaktiviteter, men jeg er usikker på om det de har gjort er i samsvar med de rettslige krav.

Pof § 2-6 stiller opp krav om at det skal etableres avvikshåndtering i organisasjonen. Pof § 2-6 første ledd stiller opp noen krav til hva som skal behandlers som avvik. Brudd på rutiner for bruk av informasjonssystemene og rene sikkerhetsbrudd, skal behandles som avvik. Rutinene skal sørge for at dersom det er forekommet uautorisert utlevering av personopplysninger der konfidensialitet er nødvendig, skal Datatilsynet varsles jf. pof § 2-6 tredje ledd. Det gis videre føring på formålet med avviksbehandlingen i pof § 2-6 annet ledd. Formålet er å gjenopprette normal tilstand, fjerne årsaken til avviket og hindre at dette skjer igjen. Det stilles også her opp et krav til dokumentasjon i pof § 2-6 fjerde ledd. Alle kommunene foretar avvikshåndtering. To av kommunene har etablert eget fagsystem for avviksrapportering. Her blir samtidig dokumentasjonskravet oppfylt. En kommune har egne skjema som blir registrert og en kommune har skjema under utarbeidelse. Hensikten med avviksrapporteringen er forstått av samtlige kommuner. Dette er viktig fordi dette gir en motivasjon til at det avvik håndteres i organisasjonen på en ordentlig måte. Selv om alle kommunene hadde innført avviksrapportering så er det usikkert om opplegget for hvordan dette gjøres er i samsvar med de rettslige kravene.

4.1.3. Samlet vurdering

Samlet sett så er de fleste aktører, roller og prosessuelle aktiviteter identifisert i alle kommuner. Ansvar etter pol som behandlingsansvarlig, som kanskje er ett av de viktigste kravene, er forstått av alle kommunene. Til tross for det har jeg ikke gått inn å vurdert alle behandlingene av personopplysninger kommunene utfører og vurdert om rett behandlingsansvarlig er definert i henhold til pol. Alle kommunene er meget opptatt av krav til sikring av personopplysninger, og ønsker å gjøre dette på en best mulig måte. Kommunene har en etablert sikkerhetsorganisasjon og en dokumentert sikkerhetsstrategi. De har også gjennomført sikkerhetsrevisjoner. Til tross for det, virker det for noen områder, og da spesielt under de prosessuelle kravene, at ikke alt er i samsvar med rettslige krav. Jeg har fått en sterk indikasjon på at alle forhold rundt risikovurdering og avvikshåndtering ikke er tilstrekkelig ivaretatt. Totalt sett så virker det som mye hos kommunene samsvarer med de rettslige kravene, men at det for noen viktige områder er en del mangler.

4.2. Faktorer som har virket styrende for organisering av informasjonssikkerhetsarbeidet.

Jeg har ovenfor sagt litt overordnet om samsvar mellom faktisk organisering og de rettslige krav. Dette er interessant i seg selv, men det som kanskje er mer interessant å se på, er hvilke faktorer som har påvirket til selve organiseringen av informasjonssikkerhetsarbeidet, og dermed bedre sikring av personopplysninger. Dette er interessant fordi hadde vi hatt mer kunnskap om dette, så vil en kunne stimulere det som påvirker mest, og med det bidra til ennå bedre sikring av personopplysninger. Dette medfører selvfølgelig samtidig til større samsvar med de rettslige krav, selv om dette i seg selv ikke er hovedhensikten. Formålet med de rettslige kravene kan hentes fra formålet med pol jf. pol § 1. Denne lyder:

Formålet med denne loven er å beskytte den enkelte mot at personvernet blir krenket gjennom behandling av personopplysninger.

Loven skal bidra til at personopplysninger blir behandlet i samsvar med grunnleggende personvernhensyn, herunder behovet for personlig integritet, privatlivets fred og tilstrekkelig kvalitet på personopplysninger.

Det er derfor viktig å ha det klart at krav i regelverk ikke skal følges kun for sin egen del. Schartum 2005 har drøftet i et notat problemstillinger rundt det å ivareta informasjonssikkerhet ved hjelp av regelverk. Hensikten med kravene i regelverkene er nettopp å sørge for bedre sikring av personopplysninger, og dermed hindre krenking av personvernet. Kravene i regelverkene skal bidra til at formålet oppnås. Det er meget interessant å vite mer om faktorer som bidrar til at formålet med lovgivning oppnås. Det er heller ikke slik at fullstendig etterlevelse av de rettslige krav alltid vil gi den beste beskyttelsen av personopplysninger. Regelverk er ikke perfekt og det kan dukke opp nye momenter i forhold til for eksempel den teknologiske utviklingen, som gjør at dagens regelverk ikke lenger er dekkende for å gi tilfredsstillende beskyttelse av personopplysninger. Dette er også en grunn til å se på faktorer som stimulerer til en bedre organisering av informasjonssikkerhetsarbeidet.

Ut fra det som jeg har funnet i mine undersøkelser er det flere faktorer som har virket styrende på organiseringen av informasjonssikkerhetsarbeidet. Disse faktorene har forskjellige egenskaper, og kan settes i forskjellige kategorier. Jeg har derfor valgt å lage tre kategorier av faktorer som sammenfaller med de tre fagområdene innen forvaltningsinformatikken. Faktorene er oppstilt i tabellen nedenfor.

Faktorer som har virket styrende på organisering av informasjonssikkerhetsarbeidet	Kategori
Lover og forskrifter	**Juridisk**
Juridisk litteratur	
Veiledninger fra Datatilsynet	
Revisjonsaktiviteter	
Etablering av personvernombud	
Utforming av sikkerhetsorganisasjon	**Organisatorisk**
Etablering av interne sikkerhetsforum	
Interkommunalt samarbeid	
Samarbeid gjennom KINS	
Tekniske standarder	**Informatisk**

Tabell 6 - Oversikt over faktorer som har virket styrende på organisering av informasjonssikkerhetsarbeidet

4.2.1. Styrende juridiske faktorer

De styrende faktorene i kommunene jeg undersøkte, var blant annet krav i lov- og forskrift. I tillegg til dette var det en forståelse av at personopplysninger måtte sikres. Det var kanskje hos personvernombudet i kommune C at jeg merket at denne interessen var mest fremtredende. Her viker selve interessen sammen med krav i lov og forskrift. Dersom ikke krav i regelverk hadde vært der så ville vi ikke kunne forvente at kommunene av eget tiltak satte i verk organisering og tiltak for å sikre ivaretakelse personopplysninger, selv om at sikkert noen tiltak for å sikre personopplysninger hadde vært iverksatt. Alle kommunene kjente til bestemmelsene i pol og pof og dette var nok den viktigste grunnen til at de hadde implementert en bestemt organisering av

informasjonssikkerhetsarbeidet relatert til sikring av personopplysninger. Selve eksistensen av krav i lov- og forskrift er derfor en meget viktig faktor for å ivareta formålet med å sikre personopplysinger og bidrar i stor grad til hvordan organiseringen gjennomføres på. Samtidig hadde kommune C brukt juridisk litteratur som veiledning til å forstå krav i lov- og forskrift.

En annen faktor som hadde betydd mye for spesielt to kommuner var veilederen fra Datatilsynet. Denne hadde fungert som mal slik at kommunene hadde tilpasset organisering og planlegge gjennomføring av de prosessuelle kravene. Veilederen inneholdt forslag til sikkerhetsstrategi og sikkerhetsmål samt mange ulike skjema for instrukser og skjema for gjennomføring av blant annet risikovurdering. Mine undersøkelser har derfor vist at denne veilederen kan være en meget viktig faktor i organiseringen av informasjonssikkerhetsarbeidet. Dersom veilederen er utformet slik at den ivaretar alle forhold rundt organiseringen av informasjonssikkerhetsarbeidet, og alle andre tiltak, vil den kunne bidra meget positivt til etterlevelse av krav i lov- og forskrift.

I to av kommunene, og spesielt i kommune A, hadde revisjonsaktiviteter spilt en vesentlig rolle og påvirking i forhold til informasjonssikkerhetsarbeidet. Revisjon er pålagt i pof § 2-5 men kommuneloven kapittel 12 omhandler også revisjon og nevner spesielt forvaltningsrevisjon i kommunelovens § 78 nr 2. Forvaltningsrevisjon omfatter normalt oppgaver, resursbruk og måloppnåelse. Her ble det gjort en del endringer i kommuneloven jf. Ot. prp. nr 70 (2002-2003) som styrket dette revisjonsarbeidet. Det er også laget en standard[131] for forvaltningsrevisjon som er en rettledning for de som skal utføre slike revisjoner. Mine undersøkelser viser at denne typen revisjonsaktiviteter også har virket styrende på organiseringen av informasjonssikkerhetsarbeidet.

Kommune C hadde etablert personvernombud etter pof § 7-12. Dette er en ordning som har sin bakgrunn i regelverket. I forkant av etableringen og i etterkant har personvernombudet jobbet mye med informasjonssikkerhet og det virker som at ordningen har stimulert til et ytterligere økt engasjement i kommunen. Dette har virket

[131] Jf. RSK 001 – Standard for forvaltningsrevisjon

styrende og hatt en meget positiv effekt på organisering av informasjonssikkerhetsarbeidet.

4.2.2. Styrende organisatoriske faktorer

Jeg var innledningsvis i kapittel 1 inne på begreper innen organisasjonsteori. Dette var organisasjonsteori som spesielt omhandlet offentlig sektor. Jeg vil i dette kapittelet drøfte de organisatoriske faktorene som har vært styrende for organiseringen av informasjonssikkerhetsarbeidet. For å gjøre dette vil jeg bruke begreper hentet fra organisasjonsteori for offentlig sektor. Christensen m.fl. 2004 beskriver det instrumentelle perspektivet på en organisasjon.[132] Her betraktes organisasjoner som redskaper eller instrumenter som er rettet mot å oppnå uttalte mål.
Undersøkelsene mine synes å vise at flere organisatoriske faktorer har hatt en positiv effekt på organiseringen om dermed bidratt til bedre sikring av personopplysninger.

Organisatorisk faktorer som har virket styrende på organisering av informasjonssikkerhetsarbeidet
Sikkerhetsorganisasjonen inkluderte interne og eksterne sikkerhetsforum
Interkommunalt samarbeid
Samarbeid gjennom KINS

Tabell 7 - Oversikt over organisatoriske styrende faktorer

Faktorene som jeg ønsker å drøfte nærmere er listet i tabellen ovenfor.
Avhengig av størrelsen på kommunen var det litt forskjell på hvor mange som var blitt gitt ansvar og myndighet og hva de forskjellige ulike personene i kommunenes organisasjon var blitt gitt av oppgaver. En kommune er en hierarkisk oppbygd organisasjon og den formelle organisasjonsstrukturen er fastlagt med rådmannen på toppen og de ulike formelle rollene i organisasjonen med tilhørende oppgaver for hver rolle. I den formelle organisasjonsstrukturen så er rollene ikke knyttet mot en bestemt person, men er upersonlige og dermed knyttet til den formelle rollen. Kravene til personelle krav som jeg definert i kapittel 2 var også upersonlige og knyttet til roller.

[132] Christensen m.fl. 2004 side 30

Siden regelverket kun identifiserer noen få roller, så vil det være opp til kommunene selv å bestemme hvordan organiseringen av informasjonssikkerhetsarbeidet skal være. Christensen m.fl. 2004 beskriver den også ulike grader og former av spesialisering og samordning som kan forekomme når en skal utforme en formell organisasjonsstruktur. En hierarkisk organisasjon innebærer ulike vertikale nivåer, en arbeidsdeling og rutiner. Arbeidsdeling innebærer at organisasjonens oppgaver blir gruppert i ulike enheter. Dersom det blir etablert ulike enheter med ulike oppgaver på samme nivå i en organisasjon kalles dette for horisontal spesialisering.[133] Hva hver enhet skal gjøre er gjerne dokumentert i form av rutiner som er nedfelt i kommunens instrukser. En hierarkisk organisasjon som en kommune kan også ha former for arbeidsdeling på ulike nivå innen organisasjonen. Dette kalles vertikal spesialisering, som for eksempel der de prinsipielle avgjørelsene innen et fagområde foretas på toppen av hierarkiet i en enhet, mens en underliggende enhet utfører mer rutinemessige oppgaver. Christensen m.fl. 2004[134] peker på at Luther Gulick[135] bruker normalt fire ulike prinsipper for horisontal spesialisering. Det første er formålsprinsippet eller sektorprinsippet der en deler sakene inn i formål- eller sektorområder. Dette er gjennomført i kommunene ved at det er delt inn i ulike sektorer som helsesektor, skolesektor, teknisk sektor etc. Det neste prinsippet er prosessprinsippet der saker fordeles etter fremgangsmåte eller type prosess. En kommune vil bruke dette prinsippet for organisering ved for eksempel en enhet som tar seg av personalsaker, en som håndterer budsjettsaker etc. Disse sakene har ikke et eget selvstendig formål men er med på å understøtte andre formål som kommunen har. Det tredje prinsippet for horisontal spesialisering er klientprinsippet. Her deles saker inn i forhold til bestemte grupper av befolkningen. En kommune vil kunne ha en egen enhet for barn og familie eller en enhet som i hovedsak skal håndtere ulike spørsmål som berører eldre. Det fjerde prinsippet kalles geografiprinsippet og innbærer at organisasjonsstrukturen er delt opp i ulike geografiske enheter. Hensikten er da å dekke oppgaver relatert til et avgrenset geografisk område. Styringsnivåene i Norge er delt opp etter dette prinsippet der det lokale styringsnivået er kommunene. Dette prinsippet brukes også av kommunene selv, der de for eksempel kan ha en kommune som er stor i

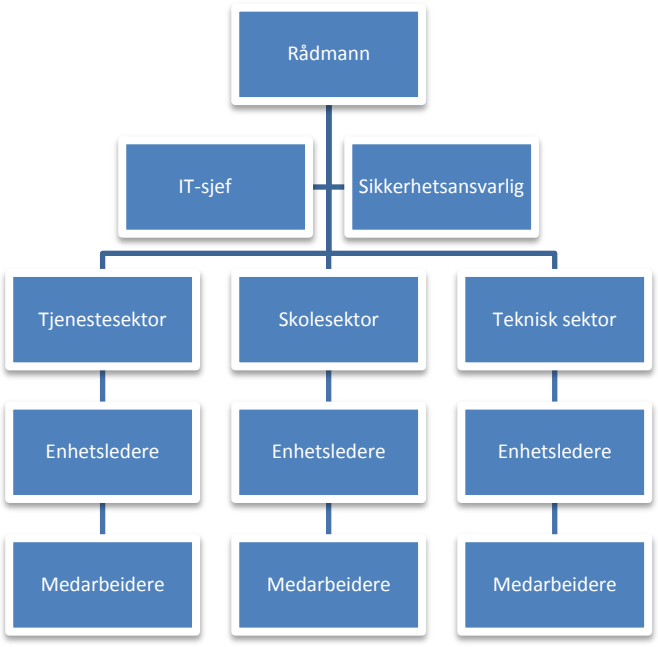
[133] Christensen m.fl. 2004 side 34
[134] Christensen m.fl. 2004 side 35
[135] Gulick, L. (1937)

utstrekning der det er delt opp i bydelsenheter. Disse prinsippene kan brukes om hverandre i en hierarkisk organisasjon, og en kan ha en kombinasjon av ulike prinsipper. Valg av prinsipper for spesialisering og samordning påvirker også informasjonsflyten i en organisasjon og vil kunne ha innvirkning på styringen og kontrollen av organisasjonen.[136] Jeg har ikke studert selve kommunens organisasjon generelt fordi dette kunne ha vært en egen oppgave i seg selv innen statsvitenskap, der en kunne ha sett på hvordan en kommunes organisasjon er strukturert på og hvilke konsekvenser dette har for kommunens evne til å oppnå sine mål. Det skal jeg ikke gjøre i denne oppgaven, men jeg skal bruke disse prinsippene for å drøfte effekter av hvordan en kommune har organisert sin sikkerhetsorganisasjon på. I tillegg til disse spesialiseringsprinsippene finnes det kollegiale strukturer som kan gå på tvers av en organisasjon der en skal oppnå horisontal samhandling mellom disse. Det kan også finnes midlertidige ordninger som utvalg og arbeidsgrupper som skal utrede konkrete problemstillinger. Disse samarbeidsformene som kalles horisontal samordning, kalles som en samlebetegnelse for nettverksstrukturer.[137] Hensikten med en bestemt organisering er å nå et mål eller løse et problem. For å nå målene etableres det også i tilegg rutiner som beskriver regler og prosedyrer for hvem som skal utføre oppgavene og hvordan de skal utføres. Kommuner har ofte mange mål og oppgaver de skal løse og er inne på at offentlige organisasjoner som kommuner er generelt har komplekse og noen ganger vage mål.[138] De må derfor gjennomføre en prioritering mellom mange ulike hensyn på en helt annen måte enn private organisasjoner. Dette gjør det mer komplekst å finne fram til en organisering som gir den høyeste måloppnåelsen. Det må ofte kombineres ulike prinsipper for spesialisering og samordning. Dette kan nok også kunne ha innvirkning på hvor høyt informasjonssikkerhet blir prioritert av kommunens ledelse og i de ulike enhetene. Jeg vil nå drøfte mulige konsekvenser av de valgte strukturene som kommunene har etablert for sin sikkerhetsorganisasjon.

Kommunene er som tidligere nevnt hierarkiske organisasjoner. Øverst i hierarkiet sitter rådmannen med det øverste ansvaret i sikkerhetsorganisasjonen. Normalt vil ikke

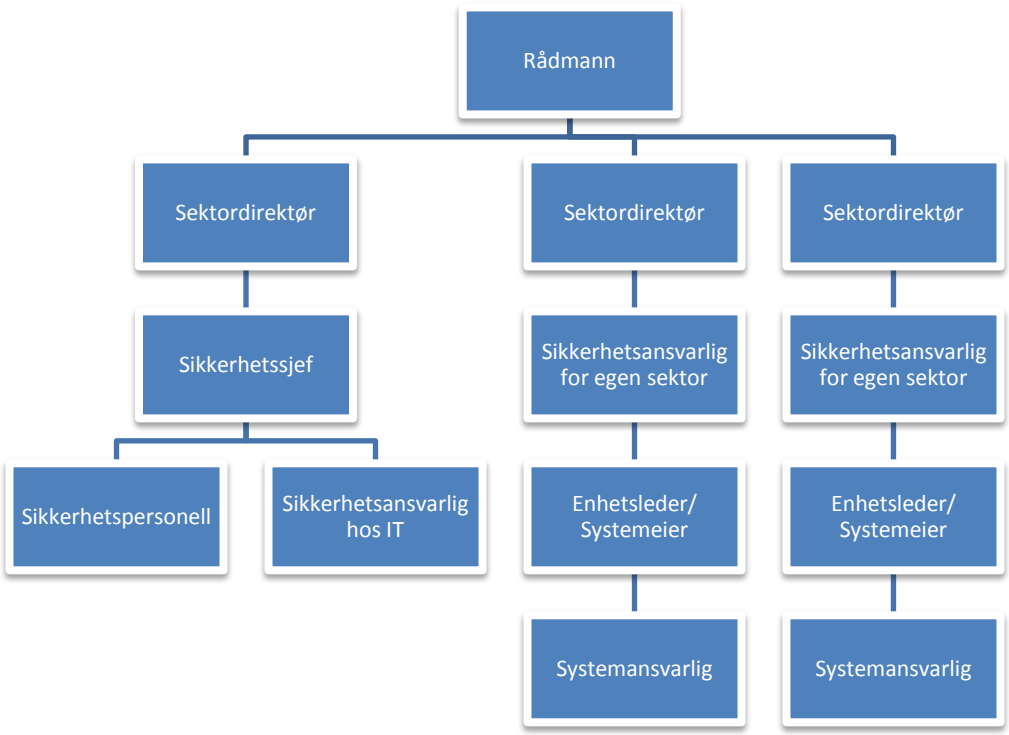
[136] Egeberg, M. 2003
[137] Christensen m.fl. 2004 side 36
[138] Christensen m.fl. 2004 side 96

rådmannen ha nok kunnskap eller tid for å ha noen utøvende oppgaver innen informasjonssikkerhetsarbeidet. Han delegerer derfor disse oppgavene nedover i sin organisasjon som innebærer en vertikal spesialisering. Avhengig av størrelse på eller andre forhold så kan det delegeres videre i organisasjonen. Dette er gjennomført i alle kommunene og ansvar for gjennomføring av oppgaver er lagt til for eksempel enhetsledere. I et par kommuner er det også ett nivå mellom enhetsleder og sikkerhetsansvarlig. I alle kommunene har også den enkelte medarbeider blant annet oppgaven med å følge fastlagte sikkerhetsrutiner. Dette medfører derfor en videre vertikal spesialisering. Alle kommunene har derfor minst 4 nivåer innen sine sikkerhetsorganisasjoner. I Kommune A har rådmannen delegert ned til IT-sjef og sikkerhetsansvarlig. Disse to er på samme nivå så her vi samtidig horisontal spesialisering med at IT-sjef har ansvar for tekniske sikkerhetstiltak og sikkerhetsansvarlig har ansvar for andre sikkerhetsoppgaver. Under disse to er det delt opp i tre sektorer, tjenestesektor, skolesektor og teknisk sektor. Under her igjen er det enhetsledere i hver sektor. Til slutt er det medarbeiderne innen hver enhet. Kommune A har derfor 4 vertikale nivåer for sin sikkerhetsorganisasjon. De har også en kombinasjon a vertikal spesialisering og så har de horisontal spesialisering etter prosessprinsippet. To av kommunene har dessuten former for horisontal samordning i tilnytning til informasjonssikkerhetsarbeidet.



Figur 2 - Oversikt over kommune A sin sikkerhetsorganisasjon

Kommune B har ennå flere nivåer. Sikkerhetssjef har delegert oppgaver fra rådmannen. Sikkerhetssjef har igjen delegert oppgaver til sikkerhetsansvarlig i egen enhet. Her har det blitt gjennomført en vertikal spesialisering på to nivåer. Videre så har sikkerhetssjef også etablert en sikkerhetsgruppe i egen enhet som skal arbeide med sikkerhet. Her er det også foretatt en horisontal spesialisering etter prosessprinsippet med at to personer i gruppen skal ha et spesielt ansvar for tekniske sikkerhetstiltak. Det er foretatt vertikal spesialisering gjennom flere nivå fra rådmann og ned til systemansvarlig. Samtidig så er sikkerhetsoppgavene fordelt på de ulike sektorene ved en horisontal spesialisering som følger kommunens ordinære organisasjon. Denne horisontale spesialisering virker fornuftig fordi de ulike fagsystemene kan være veldig forskjellige og det kan være nødvendig med god fagkunnskap for å ivareta sikkerhetsoppgaver innen hver sektor. Dette er en stor organisasjon med stor avstand mellom hver sektor. Av hensyn til for mange detaljer har jeg ikke tatt med nivået for medarbeidere, i oversiktene over sikkerhetsorganisasjonene nedenfor.

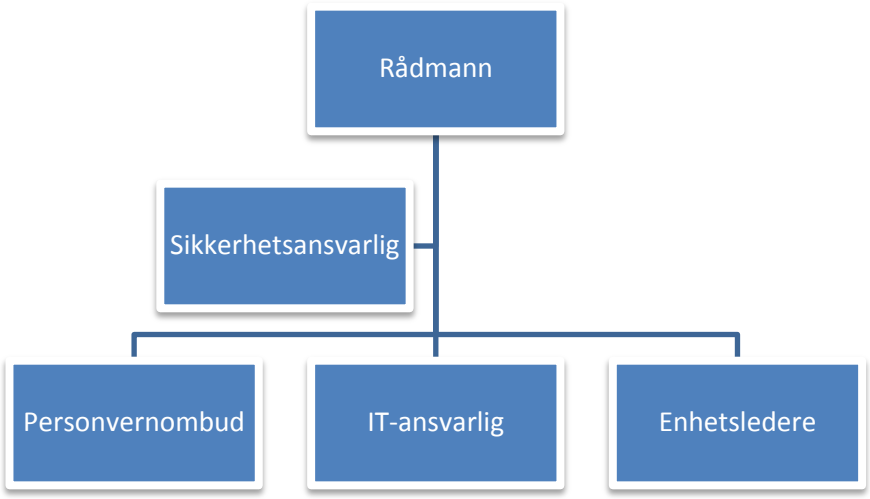


Figur 3 - Oversikt over kommune B sin sikkerhetsorganisasjon

Det er også etablert et sikkerhetsforum som ledes av sikkerhetsansvarlig hos IT-avdelingen og en sikkerhetsansvarlig fra hver sektor. Det er kun tegnet inn to sektorer men det er flere i praksis. Jeg var inne på at sikkerheten virket veldig godt ivaretatt i kommune B. Dette til tross for at de har en stor organisasjon og veldig mange fagsystemer. Når sikkersoppgaver er spredt på mange ulike personer både horisontalt og vertikalt i organisasjonen stiller dette høye krav til kommunikasjon dersom en skal få til en god styring og kontroll. At det er etablert et sikkerhetsforum som er en kollegial struktur på tvers i organisasjonen som er en horisontal samordning og som virker på meg som et meget godt tiltak for å øke sikkerhetssjefens sin mulighet for styring og kontroll på alle de delegerte sikkerhetsoppgavene. Det viser seg også i praksis at dette fungerer meget godt. Alle de prosessuelle oppgavene som jeg identifiserte blir meget godt ivaretatt i praksis. Samtidig så ble det ved gjennomføring av risikovurderinger opprettet interne arbeidsgrupper der sektoransvarlig sammen med systemeier og systemansvarlig hadde oppgaven å gjennomføre risikovurderingen. Dette er på samme måte som sikkerhetsforumet en form for nettverksstruktur som er med på å bidra til bedre måloppnåelse for kommunen.

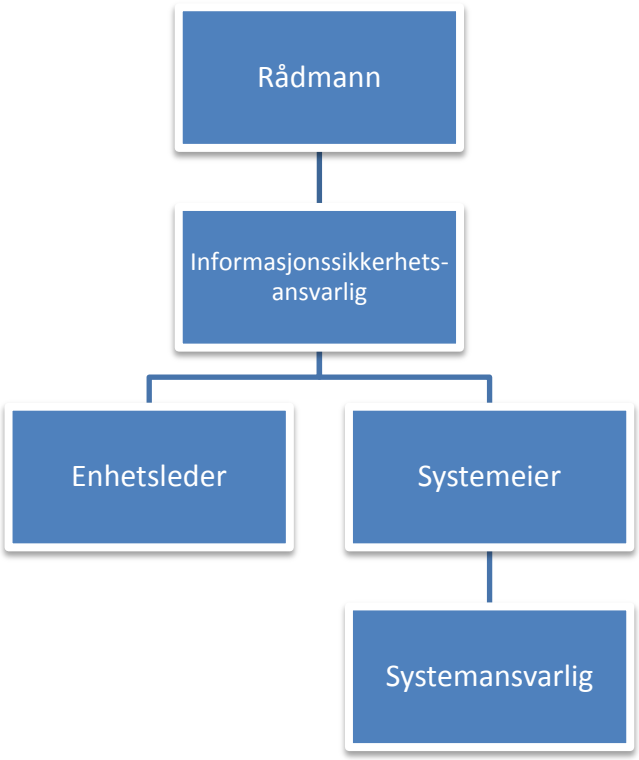
Figur 4 - Oversikt over kommune B sitt sikkerhetsforum

Kommune C hadde en litt annen organisering. De hadde foretatt en vertikal spesialisering på to nivåer der sikkerhetsansvarlig var blitt gitt ansvar og noen oppgaver mens det var videre delegert oppgaver til IT-ansvarlig og personvernombud. Samtidig var enhetslederne plassert på det samme nivået med blant annet oppgaver for opplæring av egne ansatte innen informasjonssikkerhet. På det tredje nivået hadde de her foretatt en horisontal spesialisering på samme måte som i kommune A men med enhetslederne i tillegg på samme nivået. Det å dele dette opp med direkte sikkerhetsoppgaver på 2 nivåer under rådmannen kan medføre en litt større avstand opp til rådmannen og dermed mer ufordring med styring og kontroll. For kommune C sin del så virker det som dette er kompensert for med god direkte kommunikasjon mellom rådmann og personvernombud, som ikke har fulgt den hierarkiske strukturen. Det kan tenkes at en mer effektiv organisering kunne ha vært å gjøre en organisasjonsendring ved å få til en vertikal integrasjon der ett nivå blir fjernet og alle oppgavene ble lagt på samme nivå. Dette hadde medført en organisering med horisontal spesialisering og oppdeling av oppgaver etter prosessprinsippet på tre ulike personer. Dette ville sannsynlig medført bedre styring og kontroll for rådmannen.



Figur 5 - Oversikt over sikkerhetsorganisasjonen til kommune C

Kommune D er også interessant å se spesielt på fordi de også bruker strukturer som er utenfor egen sikkerhetsorganisasjon. Sikkerhetsorganisasjonen består av rådmannen, informasjonssikkerhetsansvarlig, enhetslederne samt systemeiere med systemansvarlige. Brukerne er også definert inn under enhetslederne. Det er her foretatt en vertikal spesialisering nedover i totalt 3 nivå under rådmannen. Det er samtidig gjort en horisontal spesialisering etter prosessprinsippet der enhetslederne og systemeiere er gitt ulike konkrete oppgaver. Samtidig så er det foretatt en ytterligere vertikal spesialisering fra systemeier og ned til en systemansvarlig som har blitt gitt utøvende oppgaver.



Figur 6 - Oversikt over sikkerhetsorganisasjonen i kommune D

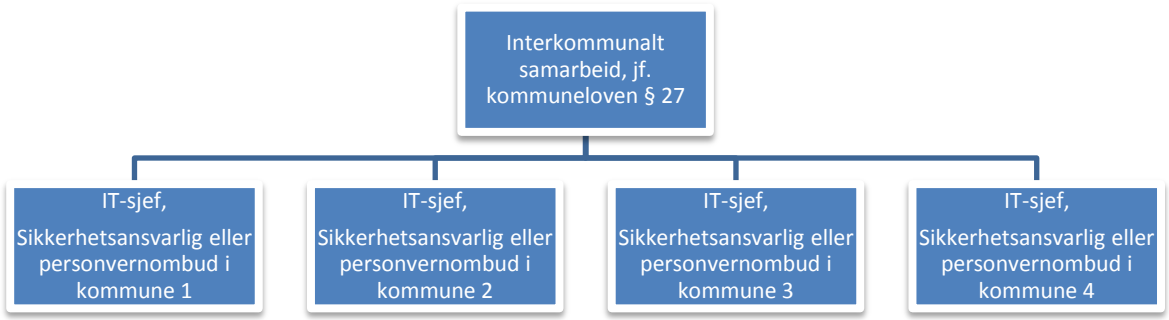
I tillegg til dette er kommune D en del av en større enhet. Det eksisterer et sikkerhetsforum på tvers av flere kommuner. Styret i det interkommunale selskapet er på toppen i hierarkiet der daglig leder i selskapet er plassert under. Videre er det en IT-sikkerhetsansvarlig i det interkommunale selskapet som også er med i sikkerhetsforumet. Daglig leder i det interkommunale selskapet leder sikkerhetsforumet. For det interkommunale selskapet sin del, så er det en ordinær vertikal spesialisering. Sikkerhetsforumet representerer en horisontal samordning for å kunne harmonisere felles

sikkerhetspolicy, sikkerhetsmål, sikkerhetsopplæring og sikkerhetstiltak i alle kommunene. Et slikt sikkerhetsforum vil være helt avgjørende for å kunne ha en enhetlig policy på området og klare å få til styring og kontroll av oppgaver. Det er også mitt inntrykk at dette fungerer godt og er en viktig del av kommunes arbeid innen informasjonssikkerhet.

Figur 7 - Oversikt over medlemmer i sikkerhetsforumet som kommune D er medlem av

Kommune C nevnte at de er med i en interkommunal[139] arbeidsgruppe som jobber spesielt med informasjonssikkerhet. Her samarbeider de og presenterer for hverandre hva de gjør og hvilke aktiviteter de har i sine respektive kommuner. Dette er et samarbeidsforum som inkluderer flere kommuner. Dette er også et eksempel på horisontal samhandling. Denne arbeidsgruppen er nok en midlertidig løsning, men jeg antar at ordningen vil eksistere så lenge kommunenes representanter mener at den er nyttig.

[139] Jf. kommuneloven § 27



Figur 8 - Interkommunalt samarbeid - arbeidsgruppe for sikkerhet

Kommune C sier at dette forumet har bidratt positivt inn i kommunens arbeid med informasjonssikkerhet og at det også har stimulert til prosesser i andre kommuner.

Alle kommunene nevner også samarbeidet gjennom Kommunal Informasjonssikkerhet (KINS). To av kommunene er medlemmer, en kommune har vært medlem og en kommune har planer om å melde seg inn. KINS er en medlemsbasert interesseorganisasjon som har som formål å bidra til økt informasjonssikkerhet i kommuner og fylkeskommuner, i tråd med slik informasjonssikkerhet blir definert i pol jf. §§ 1-3 i vedtektene til KINS. Den ene store kommunen sa at de hadde meldt seg ut av KINS og så ikke at de hadde så mye mer å hente av veiledning fra KINS. Dette kommer nok av at kommunen har mye kompetanse og har det jeg kaller en mer avansert sikkerhetsorganisasjon enn det som jeg antar er normalt for kommuner. Samtidig er nok KINS sin virksomhet mer rettet mot små og mellomstore kommuner. Dette begrunner jeg i at den ene mellomstore kommunen var medlem og den andre mellomstore ønsket å melde seg inn. KINS arrangerer konferanser og på den måten legges det til rette for å etablere mer uformelle samarbeidsfora eller uformelle strukturer eller nettverksstrukturer blant medlemmene. Dette bidrar til informasjonsutveksling og kan være med å bidra til at medlemmene av KINS blir utrustet for å få til en bedre måloppnåelse innen organisering av informasjonssikkerhetsarbeidet.

4.2.3. Styrende informatiske faktorer

Sett fra det teknologiske perspektivet så har standarder i flere tilfeller mye å si for regelverk. I forarbeidene til pol ble det drøftet om det skulle være en direkte henvisning til at sikkerhetstiltakene skulle være bygget opp i henhold til alminnelige anerkjente metoder, som også dekker tekniske standarder.[140] Det ble ikke tatt med fordi blant annet Datatilsynet mente at dette ville kunne ekskludere nye og bedre sikkerhetstiltak. Selv om det ikke kom med sier også forarbeidene at det ikke er noe til hinder for at sikkerhetstiltak blir utarbeidet i henhold til anerkjente prinsipper. I eforvaltningsforskriften er dette eksplisitt tatt med. Eforvaltningsforskriften § 13 annet ledd sier at sikkerhetsstrategien skal være utarbeidet i henhold til anerkjente prinsipper for informasjonssystemers sikkerhet. Dette gir en klar føring på at etterlevelse av tekniske standarder for informasjonssikkerhet har mye å si for etterlevelse[141] av rettslige krav. I kommentarene til pof så nevnes det at forskriften er bygget opp etter tidligere sikkerhetsregler[142] som igjen var basert på kjente teknikker og anerkjente standarder for kvalitetsstyring, internkontroll og informasjonssikkerhet. Som nevnt i tidligere så er ISO 17799 nå erstattet av ISO 27002:2005[143]. Tittelen på denne er: Informasjonsteknologi – Sikkerhetsteknikk – Administrasjon av informasjonssikkerhet. Denne standarden gir generelle veiledninger til administrasjon av informasjonssikkerhet og har fokus på sikring av informasjon generelt og informasjonssystemer. I tillegg til standarder er det også internasjonale og nasjonale retningslinjer for informasjonssikkerhet. Her kan nevnes OECD retningslinjer for sikkerhet for informasjonssystemer[144] og nettverk og nasjonale retningslinjer for å styrke informasjonssikkerheten[145]. Mange standarder og retningslinjer har som hensikt å være generelle retningslinjer som ikke skal dekke spesielle rettsområder eller samfunnssektorer, men er ment å være generelle. Dersom en kunne ha laget en sikkerhetsstandard som dekket alle aspektene for sikring av personopplysninger

[140] Ot. prp. nr. 92 (1998-99) side 115.
[141] Forholdet mellom rettslige krav til sikring av personopplysninger og forholdet til standarder er også kommentert i Jansen og Schartum 2005 side 103-104
[142] Personopplysningslovens kommentarutgave side 345
[143] NS-ISO/IEC 27002:2005
[144] http://www.oecd.org/document/42/0,3343,en_2649_34255_15582250_1_1_1_1,00.html, sist besøkt 2. juni 2009
[145] Nasjonale retningslinjer for å styrke informasjonssikkerheten 2007-2010, http://www.regjeringen.no/nb/dep/fad/dok/lover-og-regler/retningslinjer/2007/nasjonale-retningslinjer-for-informasjon.html?id=492953, sist besøkt 2. juni 2009

hadde det været veldig bra. Selv dette kunne vært ønskelig så er det nok vanskelig å lage en slik standard siden personopplysninger behandles av så veldig mange forskjellige virksomheter. Noen er veldig store og noen er veldig små. Det vil derfor være vanskelig å lage en standard som er enkel nok for de minste virksomhetene og uttømmende nok for de store.

Et eksempel på et rettsområde der det er laget standarder som skal dekke rettslige krav er innen rettslig regulering av elektronisk signatur og tilknyttede tjenester.[146] Esignaturdirektivet[147] annex II har en direkte kobling til tekniske standarder. Dette er implementert i esignaturloven[148] § 11 annet ledd som lyder:

"Kravene i første ledd skal anses oppfylte dersom sertifikatutsteder benytter seg av produkter og systemer som er godkjent av et organ i henhold til § 9 første og annet ledd, eller er i samsvar med standarder fastsatt av Europakommisjonen etter § 9 tredje ledd"

Her gis det en helt klar direkte sammenheng mellom tekniske standarder og rettslige krav. Kunngjøringen av hvilke standarder dette er gitt i annex i Kommisjonsbeslutning av 14. juli 2003[149]. Sikkerhetsstandardene det henvises til i denne kommisjonsbeslutningen er CWA[150] 14167-1 og CWA 14167-2. I annekset til kommisjonsbeslutningen listes blant annet standardene der myndigheter i medlemslandene skal gå ut fra er i samsvar med de rettslige kravene i annex II i esignaturdirektivet. Ovennevnte slår fast ar dersom en sertifikatutsteder er i samsvar med disse standardene så oppfyller de kravet i esignaturloven § 11 første ledd.

Siden dette er et helt spesielt felt og at alle som skal drive med denne typen virksomhet må ha etablert tilsvarende sikkerhet, er det mulig å lage en slik direkte kobling mellom helt konkrete standarder og rettslige krav. Det er også laget en nasjonal ordning som på

[146] Jf. Ot. prp. nr. 82 (1999-2000) side 5.
[147] Esignaturdirektivet
[148] Esignaturloven
[149] Kommisjonsbeslutning 2003/511/EC
[150] Cen Workshop Agreements, http://www.cen.eu/cenorm/businessdomains/businessdomains/isss/cen+workshop+agreements/electronic+signatures.asp, sist besøkt 2. juni 2009

en tilsvarende måte referer til en forvaltningsstandard.[151] Sammenhengen her mellom denne standarden og krav i forskrift er selvdeklarasjonsforskriften[152] § 3. Her sier selvdeklarasjonsforskriften § 3 at sertifikatutstedere skal oppfylle relevante A-krav i henhold til kravspesifikasjon for PKI i offentlig sektor. Kravene som sertifikatutstederne skal etterleve i henhold til forskriften er i denne forvaltningsstandarden[153] som FAD[154] har laget. Her er det også slik at dersom en sertifikatutsteder innretter seg slik at de er i samsvar med kravene i forvaltningsstandarden så er de dermed i samsvar med de rettslige krav.

For sikring av personopplysninger, vil en nok måtte nøye seg med at standarder er veiledende og en hjelp til etterlevelse av rettslige krav. I helsesektoren er det gjort et forsøk ved å lage norm for informasjonssikkerhet i helsesektoren.[155] Datatilsynet er også tilsyn for behandling av personopplysninger i helsesektoren og fører tilsyn etter helseregisterloven[156]. Her er det laget en omfattende norm med faktaark som dekker mange ulike delområder av informasjonssikkerhetsarbeidet. Datatilsynet har blitt forespurt om normen kan anbefales som et verktøy for etterlevelse av helseregister og pols bestemmelser i forhold til informasjonssikkerhet. Datatilsynet har svart[157] at de anser normen for å være et egnet verktøy i arbeidet for å etterleve pols og helseregisterlovens bestemmelser om informasjonssikkerhet. Dette er så langt Datatilsynet ønsker å gå. Jeg tror det derfor vil være veldig vanskelig å lage en standard for sikring av personopplysninger, der en kan erklære samsvar og dermed være i samsvar med krav i lov og forskrift.

[151] Kravspesifikasjon for PKI i offentlig sektor, http://www.regjeringen.no/nb/dep/fad/dok/rapporter_planer/rapporter/2004/kravspesifikasjon-for-pki-i-offentlig-se.html?id=106067, sist besøkt 2. juni 2009
[152] FOR 2005-11-21 nr 1296: Forskrift om frivillige selvdeklarasjonsordninger for sertifikatutstedere (Selvdeklarasjonsforskriften)
[153] At dette er en forvaltningsstandarder er beskrevet i forordet til Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor, http://www.regjeringen.no/nb/dep/fad/dok/lover-og-regler/retningslinjer/2008/rammeverk-for-autentisering-og-uavviseli.html?id=505958, sist besøkt 2. juni 2009
[154] Fornyings- og administrasjonsdepartementet (FAD)
[155] Norm for behandling av personopplysninger i helsesektoren, http://www.helsedirektoratet.no/samspill/informasjonssikkerhet/norm_for_informasjonssikkerhet_i_helsesektoren_232354, sist besøkt 2. juni 2009
[156] LOV 2001-05-18 nr 24: Lov om helseregistre og behandling av helseopplysninger (helseregisterloven)
[157] Datatilsynet, 7. august 2006, Norm for informasjonssikkerhet i helsesektoren – Datatilsynets vurdering, 05/00133-15

For kommunene sin del så var det ingen som sa de hadde hatt en utstrakt bruk av standarder som veiledning for organisering av informasjonssikkerhetsarbeidet. En kommune sa at de syntes standardene var alt for omfattende. En kommune hadde sett på noe arbeid som Larvik kommune hadde gjort i forbindelse med risikoanalyser. Kommune D hadde dessuten indirekte hatt inspirasjon fra standarder ved at firmaet som hadde utarbeidet håndboken i informasjonssikkerhet hadde brukt ISO 17799 og NS 5814 som veiledning. Mine undersøkelser viser derfor at tekniske sikkerhetsstandarder kun har hatt vært en indirekte styrende faktor innen organiseringen av informasjonssikkerhetsarbeidet i de kommunene jeg gjorde undersøkelser i.
En kan derfor si at tekniske standarder har vært en indirekte styrende faktor for organisering av informasjonssikkerhetsarbeidet, fordi de har virket styrende for utformingen av regelverket og dermed også for utformingen av veilederen fra Datatilsynet.

5. Konklusjon

I innledningen til oppgaven antydet jeg at kommuner har liten kjennskap om lover og regler som setter krav til informasjonssikkerhet. Mine undersøkelser viser at dette kanskje ikke er tilfelle. Alle fire kommuner som jeg gjorde undersøkelser i, kjente veldig godt til kravene i pol og pof. Alle var også veldig bevisst på at det var rådmannen som hadde det øverste ansvaret for behandlingen av personopplysninger i kommunen. Siden jeg kun har foretatt kvalitative studier og kun har foretatt undersøkelser i fire kommuner, kan jeg ikke generalisere og si at dette gjelder generelt for alle kommuner. Om dette er representativt for alle kommuner i Norge, vil være interessant å se på i en ny kvantitativ undersøkelse. En kunne da ha sjekket ut om alle landets kommuner har den samme kunnskapen om regelverket, som i de fire kommunene. Dersom en slik undersøkelse hadde vist at alle kommuner har slik kunnskap, ville det ha vært i motsetning til undersøkelsen foretatt av transportøkonomisk institutt i 2005.[158] Kjennskap til regelverk rundt sikring av personopplysninger, har kanskje blitt mer kjent i landets kommuner i løpet av de siste årene. Det er også andre som forsker på informasjonssikkerhet i kommuner, og inntrykket mitt bekreftes[159] av Tommy Tranvik[160] som opplever at tilstanden rundt sikring av personopplysninger i kommuner er bra. Han sier at han heller ikke har foretatt en representativ undersøkelse blant landets kommuner.

Jeg spurte innledningsvis om ”*hvilke rettslige krav gjelder for organisering av arbeidet med å sikre personopplysninger i kommuner?”* Dette resulterte i flere tabeller med rettslige krav. Jeg endte opp med å avgrense i forhold til det som jeg mente hadde mest betydning for organisering, og valgte ut rettslige krav som jeg kalte for personelle krav, det vil si der regelverkene identifiserer aktører eller roller innen informasjonssikkerhetsarbeidet. Jeg valgte også ut rettslige krav som jeg kalte prosessuelle krav, som innebar regler for hvordan enkelte sikkerhetsoppgaver skulle utføres. Disse tabellene oppsummerer etter min mening de rettslige krav som har mest

[158] TØI rapport 800/2005.
[159] http://www.forskning.no/artikler/2009/april/217225, sist besøkt 2. juni 2009.
[160] Tommy Tranvik er forsker ved Avdeling for forvaltningsinformatikk (AFIN). http://www.jus.uio.no/ifp/om/ansatte/vit/tommytr/tommytr.xml, sist besøkt 2. juni 2009

betydning for organisering av informasjonssikkerhetsarbeidet. I mine undersøkelser videre i oppgaven, brukte jeg disse rettslige kravene til å utarbeide en intervjueguide for å gjennomføre kvalitative semistrukturerte intervjuer i 4 kommuner.
Grunnen til gjennomføringen av intervjuene, var at jeg også innledningsvis spurte om *"hvordan har kommuner organisert informasjonssikkerhetsarbeidet?"* og to underspørsmål var *"hvordan er informasjonssikkerhetsarbeidet faktisk organisert"* og *"hva har reelt sett vært styrende for organiseringen av informasjonssikkerhetsarbeidet"*.
I tillegg til dette hadde jeg formulert en siste problemstilling som var *"hvilket samsvar er det mellom hvordan organiseringen faktisk er gjennomført og de rettslige kravene"*.
Den siste problemstillingen viste seg i oppgaven å være minst interessant, fordi jeg etter hvert så at det ikke var så interessant å kun se på samsvar, da dette er en oppgave som Datatilsynet blant annet har ved stedlige tilsyn. Jeg hadde dessuten ikke tilstrekkelig datamateriale for å kunne gjøre en forsvarlig rettsdogmatisk vurdering, etter gjennomførte undersøkelser i kommunene. Jeg vurderte derfor helt overordnet og gav kun en indikasjon på samsvar for kommunenes organisering av informasjonssikkerhetsarbeidet med de rettslige personelle og prosessuell kravene jeg hadde identifisert. Mine hovedfunn var at for noen av de prosessuelle kravene, var det noen mangler. Det som kanskje spesielt skilte seg ut, var noe manglede etterlevelse av alle de prosessuelle kravene til gjennomføring av risikovurdering i kommunene. Gjennomføring av risikovurdering var også et gjennomgående tema i vedtakene[161] til Datatilsynet ovenfor kommuner, der informasjonssikkerhet var nevnt spesielt. Siden Datatilsynet også i mange vedtak peker på manglende etterlevelse av dette kravet i kommuner, tør jeg generaliser og trekke den konklusjonen av dette er et område som det mangler etterlevelse hos mange norske kommuner. Dette er derfor et område som lovgiver og Datatilsynet bør se på hva som kan gjøres. De må se på hvordan en kan få til en bedre etterlevelse av rettslige krav til risikovurderinger, og dermed en bedre sikring av personopplysninger.

Det som derimot jeg synes viste seg å vært mest interessant, var hvilke faktorer som hadde vært styrende for kommunenes organisering av informasjonssikkerhetsarbeidet.

[161] Se liste over vedtak foretatt av Datatilsynet ovenfor kommuner i 2008 og 2009 i slutten av oppgaven under: Vedtak av Datatilsynet.

Her identifiserte jeg flere faktorer som hadde vært styrende. Det var forskjell på hvor stor effekt de ulike faktorene hadde hatt. Jeg syntes også det var hensiktsmessig å dele opp de styrende faktorene i juridiske, organisatoriske og informatiske faktorer. Her vurderte jeg rent skjønnsmessig om en faktor hadde hatt stor eller liten betydning.

Det viser seg at kunnskapen om hva som står i lov og forskrift er den grunnleggende årsaken til kommunenes organisering av informasjonssikkerhetsarbeidet. En annen juridisk faktor som viste seg å bety veldig mye for to av kommunene var veilederen til Datatilsynet. Mine undersøkelser har vist at veilederen har hatt mye å si for to av kommunenes organisering av informasjonssikkerhetsarbeidet. Dette hadde vært et forhold som det hadde vært veldig interessant å se på i en kvantitativ studie. Dersom mange kommuner bruker denne veilederen, kan dette være et område som Datatilsynet bør fokusere mer på, fordi dette er en faktor som da ville kunne påvirke etterlevelse av rettslige krav i stor grad.

Andre juridiske faktorer som mine undersøkelser har vist har betydning er sikkerhetsrevisjoner. Dette er allerede et rettslig krav i pof, men annet regelverk som kommuneloven har et krav til kommunerevisjon jf. kommuneloven § 78. Mine undersøkelser har vist at dette rettslige kravet i andre regelverk også virker inn på organiseringen av informasjonssikkerhetsarbeidet. Dette er også et område som jeg mener lovgiver spesielt bør se mer på. Lovgiver bør spesielt se på om det er synergieffekter som på en mer effektiv måte kan utnyttes, for å oppnå en bedre sikring av personopplysninger.

En annen juridisk faktor som har vært styrende i en kommune var etableringen av personvernombud. I pol § 7-12 står det at personvernombudet skal være uavhengig, men i dette tilfelle hadde personvernombudet utøvende oppgaver i kommunen. Hva regelverket og Datatilsynet derfor legger i begrepet uavhengig er jeg derfor usikker på. Schartum og Bygrave 2006[162] påpeker også at ordningen med personvernombud er uklar. Selv om rollen er uklar, har mine undersøkelser vist at etableringen av personvernombud fremmet

[162] Schartum og Bygrave 2006 side 38 og 128.

etterlevelse og aktiviteter rundt organiseringen av informasjonssikkerhetsarbeidet på en meget god måte. Jeg mener derfor at dette et en faktor som lovgiver og Datatilsynet bør se nærmere på for å gjøre klarere, og deretter se på hvordan det kan stimuleres til at flere kommuner etablerer personvernombud.

Av de organisatoriske faktorene som har hatt positiv styrende effekt på organiseringen av informasjonssikkerhetsarbeidet, er sikkerhetsforum i flere former. Vertikal spesialisering er fremtredende da det er nødvendig å delegere nedover i egen organisasjon ansvar for gjennomføring av praktiske oppgaver innen informasjonssikkerhetsarbeidet. Det har også vært former for horisontal spesialisering samtidig med former for horisontal samordning og da med informasjonssikkerhet som fokus. Denne kombinasjonen av horisontal spesialisering for å ivareta spesielle forhold rundt fagsystemer samtidig med horisontale samordningen i form av et sikkerhetsforum, har i mine undersøkelser vist seg å være effektivt. Det har vist seg at den horisontale samordningen på generelle sikkerhetsoppgaver har vært meget vellykket, og har stimulert den faktiske etterlevelsen av de rettslige kravene i større grad, enn der denne typen horisontal samordning ikke har vært til stede. Dette er derfor noe som bør undersøkes nærmere. Dersom en vurderer å lage nye regler med krav til organisering, vil dette kunne være en måte å organisere på, som bør tas med i betraktning.

Typen interkommunalt samarbeid der det opprettes arbeidsgrupper der personer med ansvar og oppgaver for informasjonssikkerhet, har også i mine undersøkelser vist å ha positiv innvirkning på organisering av informasjonssikkerhetsarbeidet. Dette er samarbeidsformer kommunene bør være bevisst på å utnytte. Jeg tror at kommuner kan ved å yte en liten innsats i slike fora, få mye mer igjen i form av mer samsvar med rettslige krav i egen kommune. Disse fora kan virke utdannende på disse personene som deltar, og på den måten sørge for bedre etterlevelse av rettslige krav.

Mine undersøkelser har ikke vist at tekniske standarder har vært en sterk direkte styrende faktor til bedre organisering av informasjonssikkerhetsarbeidet. Til tross for dette er tekniske standarder viktige faktorer som påvirker utforming av regelverk og som virker i

tillegg der en skal implementere generelle tiltak for informasjonssikkerhet. Som jeg nevnte ovenfor har veilederen i form av en juridisk faktor vært styrende for organisering. På en måte kan en si at denne veilederen også kan anses å være en norm eller en type løst definert standard. Det kan derfor virke som at utvikling av enkle standarder for etterlevelse av informasjonssikkerhetsregelverk kunne være en god løsning for å øke det faktiske samsvaret mellom faktisk organisering og de rettslige krav. Et eksempel på utvikling av noe som kan kalles en type standard er norm for informasjonssikkerhet innen helsesektoren.[163] Denne normen er veldig omfattende og på bakgrunn av tilbakemeldinger fra de to store kommunene, vil dette være alt for omfattende til å være brukbart for en kommune. Det var heller ingen kommuner som kommenterte at de kjente til denne normen for informasjonssikkerhet innen helsesektoren. Det kan selvfølgelig være at noen kjente til den, uten at den ble nevnt.

Denne oppgaven har vist at noen faktorer har hatt større innvirkning for organisering av informasjonssikkerhet i kommuner enn andre. Rådmenn som ofte har det daglige ansvaret, enten direkte som behandlingsansvarlig, eller som den som har det daglige ansvaret jf. pof § 2-3 første ledd, bør derfor se på de faktorene som jeg mener har hatt stor innvirkning på etterlevelse av rettslige krav, og bruke dette aktivt.

[163] http://www.helsedirektoratet.no/samspill/informasjonssikkerhet/norm_for_informasjonssikkerhet_i_helsesektoren_232354, sist besøkt 26. mai 2009

Litteraturliste

Artikkel på forskning.no	http://www.forskning.no/artikler/2009/april/217225, sist besøkt 2. juni 2009.
BS-7799-2:2002	BS-7799-2:2005 - Specification for Information Security Management (er det samme som ISO 27001:2005, jf. http://emea.bsi-global.com/InformationSecurity/Overview/index.xalter)
CWA 14167-1	Cen Workshop Agreement 14167-1 - Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements
CWA 14167-2	Cen Workshop Agreement 14167-2 - Cryptographic module for CSP signing operations with backup -Protection profile - CMCSOB PP
Datatilsynets vurdering av norm	Datatilsynet, 7. august 2006,– Datatilsynets vurdering, 05/00133-15
Egeberg, M. (2003)	Egeberg, M. (2003): ”How bureaucratic structure matters: an organisational perspective”, i B. G. Peters og J. Pierre (red.): Handbook of Public Administration. London: Sage
Erik Boe, Bind 2	Innføring i juss – Statsrett og forvaltningsrett, Erik Boe, Bind 2, Tano 1993
Erik Boe, Bind 1	Innføring i juss – Juridisk tenkning og rettskildelære, Erik Boe, Tano Aschehoug 1996, 4. opplag 2003
Gulick, L. (1937)	Gulick, L. (1937). ”Notes on the Theory of Organization”, i L. Gulick og L.F. Urwick (red.): Papers on the Science of Administration. New York: Institute of Public Administration.
Jansen og Schartum 2005	Informasjonssikkerhet, Rettslige krav til sikker bruk av IKT, Arild Jansen og Dag Wiese Schartum (red.), Faktabokforlaget 2005.
Norm for informasjonssikkerhet i helsesektoren	Norm for informasjonssikkerhet i helsesektoren, 7. august 2006.
NS 5814	NS-5814:2008 – Krav til risikovurderinger

NS-ISO/IEC 17799	NS-ISO/IEC 17799:2005, Informasjonsteknologi – Administrasjon av informasjonssikkerhet. ISO/IEC 17799 er nå erstattet av ISO/IEC 27002:2005.
NS-ISO/IEC 27002	NS-ISO/IEC 27002:2005, Informasjonsteknologi – Administrasjon av informasjonssikkerhet.
Christensen m.fl. 2004	Organisasjonsteori for offentlig sektor, Tom Christensen, Per Lægreid, Paul G. Roness, Kjell Arne Røvik, Universitetsforlaget 2004.
Personopplysningsloven s kommentarutgave	Personopplysningsloven, kommentarutgave, Johansen, Kapersen og Skullerud, Universitetsforlaget 2001
Pål Repstad 2007	Pål Repstad, Universitetsforlaget 2007, Mellom nærhet og distanse – Kvalitative metoder i samfunnsfag.
RSK 001 – Standard for forvaltningsrevisjon	RSK 001 Standard for forvaltningsrevisjon. Fastsatt av NKRFs styre 23. mai 2005 og gjort gjeldende som god kommunal revisjonsskikk forprosjekter med oppstart etter 1. oktober 2005.
Schartum og Bygrave 2004	Personvern i informasjonssamfunnet – en innføring i vern av personopplysninger, Schartum og Bygrave, Faktabokforlaget 2004
Schartum 2005	Notater om å ivareta informasjonssikkerhet ved hjelp av regelverk, Shcartum 2005, Notatet er utarbeidet som ledd i arbeid i arbeidsgruppen Regelverk og informasjonssikkerhet, nedsatt av Koordineringsutvalget for informasjonssikkerhet (KIS). Notatet er også publisert som kapittel 5 i arbeidsgruppens rapport av 7. juni 2005.
Schartum og Bygrave 2006	Schartum og Bygrave, 31. mars 2006, Utredning av behov for endringer av personopplysningsloven - Skrevet etter oppdrag fra Justisdepartementet og Moderniseringsdepartementet
Schartum 2007	Dag Wiese Schartum (red.) Elektronisk forvaltning i Norden, Praksis, Lovgivning og rettslige utfordringer, Faktabokforlaget 2007.
TØI rapport 800/2005	Behandling av personopplysninger i norske virksomheter – En spørreundersøkelse om personvern og personopplysningsloven – Inger-Anne Ravlum – TØI rapport 800/2005
Veileder i informasjonssikkerhet - Datatilsynet	Veiledning i informasjonssikkerhet for kommuner og fylker, Datatilsynet, TV-202:2005

Veileder for databehandleravtaler - Datatilsynet	Datatilsynet – Databehandleravtaler etter personopplysningsloven og helseregisterloven - Veileder 26. mai 2009

Lover, forskrifter og andre offentlige publikasjoner

eForvaltningsforskriften	Forskrift 25. juni 2004 nr. 988 om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften).
Esignaturdirektivet	Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for elektronic signatures
Esignaturloven	Lov om elektronisk signatur (esignaturloven) av 15. juni 2001 nr 81.
Forskrift av 11. april 2008 nr 345 (Deleg. til FAD etter personopplysningsloven)	Forskrift av 11. april 2008 nr 345 om Delegering av Kongen sin forskriftskompetanse etter personopplysningsloven til Fornyings- og administrasjonsdepartementet (Deleg. til FAD etter personopplysningsloven)
Forvaltningsloven	Lov 10. februar 1967 nr. 00 om behandlingsmåten i forvaltningssakter (forvaltningsloven).
Helseregisterloven	Lov om helseregistre og behandling av helseopplysninger 18. mai 2001 nr 24 (helseregisterloven).
Innst. O. nr 51 (1999-2000)	Innstillingen fra Stortingets justiskomité 22. februar 2000 i Innst. O. nr. 51 (1999-2000) om lov om behandling av personopplysninger (personopplysningsloven).
Internkontrollforskriften	Forskrift av 6. desember 1996 nr 1127 om systematisk helse-, miljø- og sikkerhetsarbeid i virksomheter (internkontrollforskriften)
Kommuneloven	Lov om kommuner og fylkeskommuner (kommuneloven) av 25. september 1992 nr 107

Kommisjonsbeslutning 2003/511/EC	Commission Decision of 14 July 2003 on the publication of reference numbers of generally recognised standards electronic signature products in accordance with Directive 1999/93/EC of the European Parliament and of the Council. (2003/511/EC)
Kravspesifikasjonen	Kravspesifikasjon for PKI i offentlig sektor versjon 1.02 januar 2005
Lov om interkommunale selskaper	Lov om interkommunale selskaper av 29. januar 1999 nr 06
NOU 1997:19	NOU 1997:19 – Et bedre personvern – forslag til lov om behandling av personopplysninger.
NOU 2009:1	NOU 2009:1 – Individ og integritet – Personvern i det digitale samfunnet. Utredning fra Personvernkommisjonen oppnevnt ved kongelig resolusjon 25. mai 2007. Avgitt til Fornyings- og administrasjonsdepartementet 13. januar 2009.
Nasjonale retningslinjer for informasjonssikkerhet	Nasjonale retningslinjer for å styrke informasjonssikkerheten 2007-2010
Ot. prp. nr. 70 (2002-2003)	Ot. prp. nr. 70 (2002-2003) Om lov om endringer i lov 25. september 1992 nr. 107 om kommuner og fylkeskommuner m.m. (kommunal revisjon).
Ot. prp. nr. 82 (1999-2000)	Ot. prp. nr. 82 (1999-2000) om lov om elektronisk signatur
Ot. prp. nr. 92(1998-99)	Ot. prp. nr. 92 (1998-99) Om lov om behandling av personopplysninger (personopplysningsloven).
Personopplysningsforskriften	Forskrift 15. desember 2000 nr 1265 om behandling av personopplysninger (personopplysningsforskriften)
Personopplysningsloven	Lov om behandling av personopplysninger (personopplysningsloven) av 14. april 2000 nr 31
Personregisterloven	Lov om personregistre m.m. (opphevet) 9. juni 1978 nr 48 (personregisterloven)
Personverndirektivet	Europaparlamentes- og rådsdirektiv 95/46/EF av 24. oktober 1995 om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger (Personverndirektivet)

Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor	Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor Retningslinjer for offentlige virksomheter som tilrettelegger elektroniske tjenester og samhandling på nett. Retningslinje 3. april 2008, Fornyings- og administrasjonsdepartementet.
Selvdeklarasjonsforskriften	FOR 2005-11-21 nr 1296: Forskrift om frivillige selvdeklarasjonsordninger for sertifikatutstedere.
St. meld. nr. 43 (2003-2004)	St. meld. nr. 43 (2003-2004) Datatilsynets og Personvernnemndas årsmeldinger for 2003
Veileder til eForvaltningsforskriften	Veileder til eForvaltningsforskriften. 20. juli 2007. Fornyings- og administrasjonsdepartementet.

Vedtak foretatt av Personvernnemnda

PVN-2007-04	PVN-2007-04 Kolumbuskortet Klage på Datatilsynets vedtak om at Rogaland Kollektivtrafikk FKF må endre løsning for etablering av elektronisk billettering for passasjerer. Personvernnemndas avgjørelse av 20. desember 2007 (Jon Bing, Gro Hillestad Thune, Lars Erik Fjørtoft, Siv Bergit Pedersen, Jostein Halgunset, Mari Bø Haugstad, Tom Bolstad)

Vedtak foretatt av Datatilsynet

Datatilsynet – 08/00231	Vedtak – Endelig kontrollrapport etter kontroll hos Bø kommune – ACOS AS
Datatilsynet – 08/00238	Vedtak om pålegg – Endelig kontrollrapport etter kontroll ved Kommuneforlaget
Datatilsynet – 08/00251	Vedtak om pålegg – Endelig kontrollrapport for Molde kommune
Datatilsynet – 08/00252	Vedtak om pålegg – Endelig kontrollrapport for Elverum kommune
Datatilsynet – 08/00254	Vedtak om pålegg – Endelig kontrollrapport – Kontroll hos Stange kommune
Datatilsynet – 08/00306	Vedtak om pålegg – Endelig kontrollrapport Tromsø kommune

Datatilsynet – 08/00307	Vedtak om pålegg – Endelig kontrollrapport Sarpsborg kommune
Datatilsynet – 08/00308	Vedtak om pålegg – Endelig kontrollrapport for Ørskog kommune
Datatilsynet – 08/00309	Vedtak om pålegg – Endelig kontrollrapport Orkdal kommune
Datatilsynet – 08/00310	Vedtak om pålegg – Endelig kontrollrapport Dovre kommune
Datatilsynet – 08/00342	Vedtak om pålegg – Endelig kontrollrapport for Stavanger kommune
Datatilsynet – 08/00353	Vedtak om pålegg – Endelig kontrollrapport for Bærum kommune
Datatilsynet – 08/00414	Vedtak om pålegg – Endelig kontrollrapport for Nøtterøy kommune
Datatilsynet – 08/00418-5	Vedtak om pålegg – Endelig kontrollrapport for Lørenskog kommune
Datatilsynet – 08/01457	Vedtak om pålegg – Endelig kontrollrapport for Hordaland fylkeskommune
Datatilsynet – 08/01458	Vedtak om pålegg – Endelig kontrollrapport for Oppland fylkeskommune
Datatilsynet – 08/01497	Vedtak om pålegg og endelig kontrollrapport etter kontroll hos Akershus fylkeskommune - Læringsplattformer
Datatilsynet – 08/01498	Vedtak om pålegg og endelig kontrollrapport – Drømtorp videregående skole – Akershus fylkeskommune
Datatilsynet – 08/01499	Vedtak om pålegg og endelig kontrollrapport hos Hedmark fylkeskommune – Bruk av læringsplattform
Datatilsynet – 08/01505	Vedtak og endelig kontrollrapport etter kontroll ved Eiker videregående skole – Buskerud fylkeskommune
Datatilsynet – 09/00180	Vedtak og endelig kontrollrapport etter kontroll hos Notodden kommune
Datatilsynet – 09/00182	Vedtak og endelig kontrollrapport etter kontroll hos Ås kommune
Datatilsynet – 09/00183	Vedtak og endelig kontrollrapport etter kontroll hos Moss kommune
Datatilsynet – 09/00184	Vedtak og endelig kontrollrapport etter kontroll hos Nittedal kommune

Oversikt over vedlegg

Tabelliste

Figurliste

Muntlige kilder/intervju

Intervju av IT-sjef i kommune A gjennomført 2. april 2009.

Intervju av IT-sjef/sikkerhetsjef i kommune B gjennomført 20. april 2009.

Intervju av personvernombud i kommune C gjennomført 27. april 2009.

Intervju av IKT-rådgiver/informasjonssikkerhetsansvarlig i kommune D gjennomført 11. mai 2009.

Annen dokumentasjon fra kommuner

(Fullstendig tittel for noe av dokumentasjonen er forenklet slik at den enkelte kommune ikke kan identifiseres)

Kommune A

- Informasjonssikkerhetsdokument
- Forslag til prosedyrer for gjennomføring av risiko- og sårbarhetsanalyse knyttet til tele- og ekomtjenester.
- Sikkerhetsinstruks bruker
- Rapport etter forvaltningsrevisjon – IKT-sikkerhet og sårbarhet.

Kommune C

- Sikkerhetsstrategi
- Oversikt over alle behandlinger av personopplysninger
- Skjema for registrering av risiko og sårbarhet.
- Driftsrutiner
- Avvikshåndtering
- Sikkerhetsinstruks for sikkerhetsansvarlig
- Sikkerhetsinstruks for bruker
- Oversikt over sikkerhetsorganisasjonen
- Databehandleravtale
- Instruks for bruk av Internett,
- Instruks for behandling av e-postkasser og private filer ved avsluttet arbeidsforhold
- Instruks for innsyn i e-post
- Instruks for bruk av e-post
- Rutiner ved ansettelse/opphør av arbeidsforhold
- Instruks for bruk av bærbart utstyr
- Instruks for bruk av hjemmekontor

Kommune D

Håndbok i informasjonssikkerhet som blant annet inneholdt:

- Sikkerhetsmål og sikkerhetsstrategi
- Registeroversikt med konsesjoner, hjemmel og plassering
- Revisjonsguide for sikkerhetsrevisjon
- Rapport for sikkerhetsrevisjoner
- Rapport fra risikoanalyser
- Skjema for gjennomføring av risikoanalyse
- Rapportskjema for risikovurdering
- Mal for rapport fra ledelsen gjennomgang
- Skjema for å autorisere bruker til nettverket
- Taushetserklæring for leverandører og partnere
- Sjekkliste og skjema for oppkobling av andre til nettverket
- Kontrakt for oppkobling av leverandører og partnere til nettet
- Kontrakt for bruk av hjemmekontorløsning
- Skjema for endring av brannmurene
- Skjema for innhenting av informert samtykke
- Skjema for avviksbehandling og erfaringstilbakeføring

Kategori 1 - Personelle krav	Kategori 2 - Materielle krav	Kategori 3 - Prosessuelle krav	Referanse	Merknader
behandlingsansvarlig			§ 2 nr 4	Kun legaldefinisjon og det knyttes ikke ansvar eller oppgaver til rollen her.
databehandler			§ 2 nr 5	Kun legaldefinisjon og det knyttes ikke ansvar eller oppgaver til rollen her.
en representant som er etablert i Norge			§ 4 tredje ledd	Dersom en behandlingsansvarlig er etablert i stater utenfor EØS-området og benytter hjelpemidler i Norge skal den behandlingsansvarlige ha en representant som er etablert i Norge, jf § 4 annet og tredje ledd.
Den behandlingsansvarlige og databehandleren	sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger	gjennom planlagte og systematiske tiltak	§ 13 første ledd	
Den behandlingsansvarlige og databehandleren	for å oppnå tilfredsstillende informasjonssikkerhet	dokumentere informasjonssystemet og sikkerhetstiltakene	§ 13 annet ledd første punktum	Her er det en oppgave som skal gjennomføres og vil da normalt ligge i kategori 2. Siden dokumentasjon i dette tilfelle er en metode for å oppnå en målsetning (tilfredsstillende informasjonssikkerhet) er det å dokumentere her lagt i kategori 3

Den behandlingsansvarlige og databehandleren	Dokumentere informasjonssystemet og sikkerhetstiltakene		§ 13 annet ledd første punktum	
Den behandlingsansvarlige og databehandleren	Dokumentasjonen skal være tilgjengelig for medarbeidere hos den behandlingsansvarlige og host databehandleren		§ 13 annet ledd annet punktum	
En behandlingsansvarlig	som lar andre få tilgang til opplysninger … skal påse at disse (databehandler eller andre) oppfyller kravene i § 13 første og annet ledd.		§ 13 tredje ledd	
Kongen	kan gi forskrift om informasjonssikkerhet … herunder nærmere regler om organisatoriske og tekniske sikkerhetstiltak.		§ 13 fjerde ledd	

Den behandlingsansvarlige	skal etablere og holde vedlike planlagte og systematiske tiltak som er nødvendige for å oppfylle kravene i eller i medhold av denne loven		§ 14 første ledd	Dette er hovedregelen og planlagte og systematiske tiltak etter § 13 første ledd er et spesialtilfelle av internkontroll. Jf. Ot. prp. nr. 92 (1998-99) paragraf 9.6.
Den behandlingsansvarlige	dokumentere tiltakene		§ 14 annet ledd	
Den behandlingsansvarlige	Gjøre dokumentasjon tilgjengelig for medarbeidere hos den behandlingsansvarlige og hos databehandler		§ 14 annet ledd	
En databehandler	kan ikke behandle personopplysninger på annen måte enn det som er skriftlig avtalt med den behandlingsansvarlige	på annen måte enn det som er skriftlig avtalt	§ 15 første ledd første punktum	Her er det plassert en bisetning i kategori 3 fordi denne gir informasjon om hvordan en databehandler skal behandle personopplysninger. Den videre beskrivelsen av hvordan behandling skal gjennomføres på skal beskrives i en avtale.
databehandler		Opplysningene kan heller ikke uten slik avtale overlates til noen andre for lagring eller bearbeidelse.	§ 15 første ledd annet punktum	Setningen gir en beskrivelse av hvordan behandling av personopplysninger skal foretas av en databehandler.

		I avtalen med den behandlingsansvarlige skal det også gå frem at databehandleren plikter å gjennomføre slike sikringstiltak som følger av § 13.	§ 15 annet ledd	Plikten til å gjennomføre sikringstiltak er plassert i kategori 2 i nedenfor.
databehandler	… databehandleren plikter å gjennomføre slike sikringstiltak som følger av § 13.		§ 15 annet ledd	Implisitt
Hvem som har det daglige ansvaret	for å oppfylle den behandlingsansvarliges plikter		§ 18 første ledd bokstav b	
Hvem som har det daglige ansvaret	for å oppfylle den behandlingsansvarliges plikter		§ 32 første ledd bokstav c	

Kategori 1 - Personelle krav	Kategori 2 - Materielle krav	Kategori 3 - Prosessuelle krav	Referanse	Merknader
		Der slik fare (etter første ledd) er til stede skal de planlagte og systematiske tiltakene som treffes i medhold av forskriften, stå i forhold til sannsynligheten for og konsekvens av sikkerhetsbrudd	§ 2-1 andre ledd	Gir føringer på hvilken måte og omfang (hvordan) de planlagte og systematiske tiltakene skal implementeres, jf. pol § 13 første ledd, jf. "tilfredsstillende".
Datatilsynet	kan gi pålegg om sikring av personopplysninger og herunder fastlegge kriterier for akseptabel risiko forbundet med behandlingen av personopplysninger		§ 2-2	Er ikke sikker på om jeg skal ta med denne da denne ikke gir kompetanse til virksomheten som er behandlingsansvarlig, men til Datatilsynet.
Den som har den daglige ledelsen av virksomheten som den behandlingsansvarlige driver	har ansvar for at bestemmelsene i dette kapittelet følges.		§ 2-3 første ledd	
	overordnede føringer for bruk av informasjonsteknologi skal beskrives i sikkerhetsmål		§ 2-3 annet ledd	
		Valg og prioriteringer i sikkerhetsarbeidet skal beskrives i en sikkerhetsstrategi.	§ 2-3 tredje ledd	Er plasserte i kategori 3 fordi denne bestemmelsen sier noe om hvordan sikkerhetsarbeidet skal gjennomføres. Sikkerhetsstrategien omfatter også beslutninger om organisering av sikkerhetsarbeidet, jf. veiledning til pof til § 2-3.

	Bruk av informasjonssystemet skal jevnlig gjennomgås	for å klarlegge om den er hensiktmessig i forhold til virksomhetens behov, og om sikkerhetsstrategien gir tilfredsstillende informasjonssikkerhet som resultat	§ 2-3 fjerde ledd	
	Resultatet fra gjennomgangen skal dokumenteres	Resultatet fra gjennomgangen skal dokumenteres og benyttes som grunnlag for eventuell endring av sikkerhetsmål og strategi.	§ 2-3 femte ledd	
	Det skal føres oversikt over hva slags personopplysninger som behandles.		§ 2-4 første ledd	
Virksomheten	Virksomheten skal selv fastlegge kriterier for akseptabel risiko forbundet med behandlingen av personopplysninger.		§ 2-4 første ledd	
Den behandlingsansvarlige	skal gjennomføre risikovurdering for å klarlegge sannsynligheten for og konsekvenser av sikkerhetsbrudd	Ny risikovurdering skal gjennomførers ved endringer som har betydning for informasjonssikkerheten.	§ 2-4 annet ledd	
		Resultatet av risikovurderingen skal sammenlignes med de fastlagte kriterier for akseptabel risiko forbundet med behandling av personopplysninger.	§ 2-4 tredje ledd	

	Resultatet av risikovurderingen skal dokumenteres		§ 2-4 fjerde ledd	I lys av hva som sies i pol § 13 at det å dokumentere sikkerhetstiltak er en måte å oppnå tilfredsstillende informasjonssikkerhet, kan dokumentasjonskravet også kunne bli plassert i kategori 3.
Implisitt en sikkerhetsrevisor	Sikkerhetsrevisjon av bruk av informasjonssystemet skal gjennomføres jevnlig	gjennomføres jevnlig	§ 2-5 første ledd	
kommunikasjonspartner og leverandør		Sikkerhetsrevisjon skal omfatte vurdering av organisering, sikkerhetstiltak og bruk av kommunikasjonspartner og leverandører.	§ 2-5 annet ledd	
		Dersom sikkerhetsrevisjonen avdekker bruk av informasjonssystemet som ikke er forutsatt, skal dette behandler som avvik, jf § 2-6.	§ 2-5 tredje ledd	Er plassert i kategori 3 fordi det beskrives hvordan deler av prosessen med å utføre sikkerhetsrevisjon skal utføres.
	Resultatet fra sikkerhetsrevisjon skal dokumenteres		§ 2-5 fjerde ledd	I lys av hva som sies i pol § 13 at det å dokumentere sikkerhetstiltak er en måte å oppnå tilfredsstillende informasjonssikkerhet, kan dokumentasjonskravet også kunne bli plassert i kategori 3.
		Bruk av informasjonssystemet som er i strid med fastlagte rutiner, og sikkerhetsbrudd, skal behandles som avvik.	§ 2-6 første ledd	

	Avviksbehandling skal gjennomføres	Avviksbehandlingen skal ha som formål å gjenopprette normal tilstand, fjerne årsaken til avviket og hindre gjentagelse.	§ 2-6 annet ledd	
		Dersom avviket har medført uautorisert utlevering av personopplysninger hvor konfidensialitet er nødvendig, skal Datatilsynet varsles.	§ 2-6 tredje ledd	
	Resultatet fra avviksbehandling skal dokumenteres		§ 2-6 fjerde ledd	I lys av hva som sies i pol § 13 at det å dokumentere sikkerhetstiltak er en måte å oppnå tilfredsstillende informasjonssikkerhet, kan dokumentasjonskravet også kunne bli plassert i kategori 3.
		Det skal etableres klare ansvars- og myndighetsforhold for bruk av informasjonssystemet	§ 2-7 første ledd	
	Ansvars- og myndighetsforhold skal dokumenteres		§ 2-7 annet ledd	I lys av hva som sies i pol § 13 at det å dokumentere sikkerhetstiltak er en måte å oppnå tilfredsstillende informasjonssikkerhet, kan dokumentasjonskravet også kunne bli plassert i kategori 3.
behandlingsansvarliges daglige leder		Ansvars- og myndighetsforhold skal ikke endres uten autorisasjon fra den behandlingsansvarliges daglige leder.	§ 2-7 annet ledd	Sier noe om hvordan ansvars- og myndighetsforhold skal gjennomføres

	Informasjonssystemet skal konfigureres		§ 2-7 tredje ledd	
		Informasjonssystemet skal konfigureres slik at tilfredsstillende informasjonssikkerhet oppnås.	§ 2-7 tredje ledd	
	Konfigurasjonen skal dokumenteres		§ 2-7 fjerde ledd	I lys av hva som sies i pol § 13 at det å dokumentere sikkerhetstiltak er en måte å oppnå tilfredsstillende informasjonssikkerhet, kan dokumentasjonskravet også kunne bli plassert i kategori 3.
den behandlingsansvarliges daglige leder		Konfigurasjonen skal ikke endres uten autorisasjon fra den behandlingsansvarliges leder.	§ 2-7 fjerde ledd	
		Bruk av informasjonssystemet som har betydning for informasjonssikkerheten, skal utføres i henhold til fastlagte rutiner.	§ 2-7 femte ledd	
	Det skal etableres fastlagte rutiner for bruk av informasjonssystemet		§ 2-7 femte ledd	Denne oppgaven gis her som et implisitt krav
Medarbeidere hos den behandlingsansvarlige		skal bare bruke informasjonssystemet for å utføre pålagte oppgaver, og selv være autorisert for slik bruk.	§ 2-8 første ledd	
Medarbeiderne		skal ha nødvendig kunnskap for å bruke informasjonssystemet i samsvar med de rutiner som er fastlagt	§ 2-8 annet ledd	

	Autorisert bruk av informasjonssystemet skal registreres	Autorisert bruk av informasjonssystemet skal registreres	§ 2-8 tredje ledd	Dette er en oppgave men samtidig sier dette kravet også noe om hvordan rutiner for bruk av informasjonssystemet skal implementeres.
Medarbeidere	Medarbeidere hos den behandlingsansvarlige skal pålegges taushetsplikt for personopplysninger hvor konfidensialitet er nødvendig.	Taushetsplikten skal også omfatte annen informasjon med betydning for informasjonssikkerheten	§ 2-9	
	Det skal treffes tiltak mot uautorisert adgang til utstyr som brukes for å behandle personopplysninger etter forskriften her.		§ 2-10 første ledd	
		Sikkerhetstiltakene skal også hindre uautorisert adgang til annet utstyr av betydning for informasjonssikkerheten	§ 2-10 annet ledd	
		Utstyr skal installeres slik at ikke påvirkning fra driftsmiljøet får betydning for behandlingen av personopplysninger.	§ 2-10 tredje ledd	
	Det skal treffes tiltak mot uautorisert innsyn i personopplysninger hvor konfidensialitet er nødvendig.		§ 2-11 første ledd	
	Sikkerhetstiltakene skal også hindre uautorisert innsyn i annen informasjon med betydning for		§ 2-11 annet ledd	Er litt usikker på plassering her. Kan også muligens plasseres i kategori 3

	informasjonssikkerheten.			
		Personopplysninger som overføres elektronisk ved hjelp av overføringsmedium utenfor den behandlingsansvarliges fysiske kontroll, skal krypteres eller sikres på annen måte når konfidensialitet er nødvendig.	§ 2-11 tredje ledd	
		For lagringsmedium som inneholder personopplysninger hvor konfidensialitet er nødvendig, skal behovet for sikring av konfidensialitet fremgå ved hjelp av merking eller på annen måte	§ 2-11 fjerde ledd	
		Dersom lagringsmediet ikke lenger benyttes for behandling av slike opplysninger, skal opplysningene slettes fra lagringsmediet	§ 2-11 femte ledd	
	Det skal treffes tiltak for å sikre tilgang til personopplysninger hvor tilgjengelighet er nødvendig		§ 2-12 første ledd	
	Sikkerhetstiltakene skal også sikre tilgang til annen informasjon med betydning for informasjonssikkerheten		§ 2-12 annet ledd	Er litt usikker på plassering her. Kan også muligens plasseres i kategori 3

	Alternativ behandling skal forberedes	Alternativ behandling skal forberedes for de tilfeller informasjonssystemet er utilgjengelig for normal bruk	§ 2-12 tredje ledd	Også plassert i kategori 3 siden det sies noe om hvordan alternativ behandling skal gjennomføres
	Personopplysninger og annen informasjon som er nødvendig for gjenoppretting av normal bruk, skal kopieres	Personopplysninger og annen informasjon som er nødvendig for gjenoppretting av normal bruk, skal kopieres	§ 2-12 fjerde ledd	Plassert i begge kategorier siden oppgaven går ut på at informasjon skal kopieres mens kravet går også ut på å beskrive rutiner for hvordan tilgjengelighet skal oppnås.
	Det skal treffes tiltak mot uautorisert endring av personopplysninger der integritet er nødvendig.		§ 2-13 første ledd	
	Sikkerhetstiltakene skal også hindre uautorisert endring av annen informasjon med betydning for informasjonssikkerheten		§ 2-13 annet ledd	
	Det skal treffes tiltak mot ødeleggende programvare		§ 2-13 tredje ledd	
		Sikkerhetstiltak skal hindre uautorisert bruk av informasjonssystemet og gjøre det mulig å oppdage forsøk på slik bruk	§ 2-14 første ledd	
	Forsøk på uautorisert bruk av informasjonssystemet skal registreres.	Forsøk på uautorisert bruk av informasjonssystemet skal registreres.	§ 2-14 annet ledd	Plassert i begge kategorier siden kravet også sier noe om hvordan sikkerhetstiltak for informasjonssystemet skal gjennomføres

		Sikkerhetstiltak skal omfatte tiltak som ikke kan påvirkes eller omgås av medarbeiderne, og ikke være begrenset til handlinger som den enkelte forutsettes å utføre.	§ 2-14 tredje ledd	
	Sikkerhetstiltak skal dokumenteres		§ 2-14 fjerde ledd	I lys av hva som sies i pol § 13 at det å dokumentere sikkerhetstiltak er en måte å oppnå tilfredsstillende informasjonssikkerhet, kan dokumentasjonskravet også kunne bli plassert i kategori 3.
Den behandlingsansvarlige	skal bare overføre personopplysninger elektronisk til den som tilfredsstiller kravene i forskriften her		§ 2-15 første ledd	Er litt usikker på plassering her. Kan også muligens plasseres i kategori 3
Den behandlingsansvarlige		kan overføre personopplysninger til enhver dersom overføringen skjer i samsvar med reglene i personopplysningsloven §§ 29 og 30, eller når det er fastsatt i lov at det er adgang til å kreve opplysninger fra et offentlig register	§ 2-15 annet ledd	
Leverandører	som gjennomfører sikkerhetstiltak, eller gjør annen bruk av informasjonssystemet på den behandlingsansvarliges vegne, skal tilfredsstille kravene i dette kapittelet.		§ 2-15 tredje ledd	

Den behandlingsansvarlige	skal etablere klare ansvars- og myndighetsforhold overfor kommunikasjonspartnere og leverandører.		§ 2-15 fjerde ledd	
kommunikasjonspartner og leverandør	Den behandlingsansvarlige skal etablere klare ansvars- og myndighetsforhold overfor kommunikasjonspartnere og leverandører		§ 2-15 fjerde ledd	
	Ansvars- og myndighetsforhold skal beskrives i særskilt avtale	Ansvars- og myndighetsforhold skal beskrives i særskilt avtale	§ 2-15 fjerde ledd	Plassert i begge kategorier fordi oppgaven går ut på at ansvars- og myndighetsforhold skal beskrives og det prosessuell går ut på at det skal beskrives i en særskilt avtale.
Den behandlingsansvarlige	skal ha kunnskap om sikkerhetsstrategien hos kommunikasjonspartnere og leverandører	og jevnlig forsikre seg om at strategien gir tilfredsstillende informasjonssikkerhet	§ 2-15 femte ledd	
kommunikasjonspartner og leverandør	Den behandlingsansvarlige skal ha kunnskap om sikkerhetsstrategien hos kommunikasjonspartnere og leverandører		§ 2-15 femte ledd	
	Rutiner for bruk av informasjonssystemet og annen informasjon med betydning for informasjonssikkerheten, skal dokumenteres		§ 2-16 første ledd	Her er det et eksplisitt krav til å utarbeide rutinedokumentasjon som ofte kalles instrukser. Jf. også det implisitte kravet i forskriften § 2-7 femte ledd

		Dokumentasjonen skal lagres i minst 5 år fra det tidspunkt dokumentet ble erstattet med ny gjeldende utgave	§ 2-16 annet ledd	
		Registrering av autorisert bruk av informasjonssystemet og av forsøk på uautorisert bruk, skal lagres minst 3 måneder. Det samme gjelder registrering av alle andre hendelser med betydning for informasjonssikkerheten.	§ 2-16 tredje ledd	
Den behandlingsansvarlige	skal etablere internkontroll i samsvar med personopplysningsloven § 14.	De systematiske tiltakene skal tilpasses virksomhetens art, aktiviteter og størrelse i det omfang det er nødvendig for å etterleve krav gitt i eller i medhold av personopplysningsloven, med særlig vekt på bestemmelser gitt i medhold av personopplysningsloven § 13	§ 3-1 første ledd	
behandlingsansvarlige	Internkontroll innebærer at den behandlingsansvarlige blant annet skal sørge for å ha kjennskap til gjeldende regler om behandling av personopplysninger, tilstrekkelig og oppdatert dokumentasjon for gjennomføring av de ovenstående rutiner, samt ha denne dokumentasjonen tilgjengelig for de den måtte angå.		§ 3-1 annet ledd	Siden krav til sikring av personopplysninger faller inn under bestemmelsen om internkontroll vil det derfor her gjelde disse materielle kravene også for sikring av personopplysninger

uavhengig personverneombud	har i oppgave å sikre at den behandlingsansvarlige følger personopplysningsloven med forskrift		§ 7-12	Dette medfører at det uavhengige personvernombudet, dersom det blir oppnevnt, også har som oppgave å påse at kravene til sikring av personopplysninger blir fulgt.

Kategori 1 - Personelle krav	Kategori 2 - Materielle krav	Kategori 3 - Prosessuelle krav	Referanse	Merknader
Enhver som utfører tjeneste eller arbeid for et forvaltningsorgan,	plikter å hindre at andre får adgang eller kjennskap til det han i forbindelse med tjenesten eller arbeidet får vite om: 1) noens personlige forhold		§ 13 første ledd nr 1	
Enhver som utfører tjeneste eller arbeid for et forvaltningsorgan,	Taushetsplikten	Taushetsplikten gjelder også etter at vedkommende har avsluttet tjenesten eller arbeidet.	§ 13 tredje ledd	Gir utfyllende beskrivelser om hvordan taushetsplikten skal forstås.
	Taushetsplikten	Taushetsplikt etter § 13 er ikke til hinder for:	§ 13 a	Når det ikke er behov for beskyttelse
	Taushetsplikten	Taushetsplikt etter § 13 er ikke til hinder for:	§ 13 b	Ut fra private eller offentlige interesser
Vedkommende forvaltningsorgan	skal sørge for at taushetsplikten blir kjent	Kan kreve skriftlig erklæring om at de kjenner og vil respektere reglene	§ 13 c første ledd	
forvaltningsorganet	Dokumenter og annet materiale som inneholder opplysninger undergitt taushetsplikt, skal forvaltningsorganet oppbevare på betryggende måte.		§ 13 c annet ledd	

departementet	kan bestemme fritak for taushetsplikt for opplysninger til bruk for forsking	Til vedtak som nevnt i første ledd kan det knyttes vilkår. Disse kan bl.a. gi bestemmelser om hvem som skal ha ansvar for opplysningene og hvem som skal ha adgang til dem, om oppbevaring og tilbakelevering av utlånt material, om tilintetgjøring av avskrifter, om hvorvidt forskere skal ha adgang til å henvende seg til eller innhente nærmere opplysninger om dem det er gitt opplysninger om, og om bruken av opplysningene for øvrig.	§ 13 d	
Enhver som utfører tjeneste eller arbeid for et forvaltningsorgan,	Dersom noen som utfører tjeneste eller arbeid for et forvaltningsorgan, er pålagt taushetsplikt ved bestemmelse i annen lov, forskrift eller instruks av hensyn til private interesser	gjelder §§ 13 til 13 e som utfyllende regler når ikke annet er bestemt i lov eller i medhold av lov.	§ 13 f første ledd	

	Taushetsplikten	Bestemmelse i annen lov om rett eller plikt til å gi opplysninger begrenser ikke lovbestemt taushetsplikt.	§ 13 f annet ledd	
Kongen	kan gi forskrift om elektronisk kommunikasjon mellom forvaltningen og publikum og elektronisk saksbehandling og kommunikasjon i forvaltningen, herunder nærmere regler om:		§ 15 a første ledd	
	signering, autentisering, sikring av integritet og konfidensialitet		§ 15 a første ledd b)	
	krav til de produkter, tjenester og standarder som kan benyttes		§ 15 a første ledd d)	
	forvaltningens rett til å sperre for brukere som misbruker data ment for signering, autentisering, sikring av integritet eller konfidensialitet, og hva som skal regnes som misbruk.		§ 15 a første ledd e)	

Kategori 1 - Personelle krav	Kategori 2 - Materielle krav	Kategori 3 - Prosessuelle krav	Referanse	Merknader
Enhver	Ved henvendelser	Kan henvende seg til et forvaltningsorgan uten bruk av sikkerhetstjenester- eller produkter, med mindre bruk av slike sikkerhetstjenester- og produkter er nødvendig for å oppfylle krav fastsatt i henhold til § 4 nr (2)-(3) eller som følger av § 5, eller krav fastsatt i annen lov eller i medhold av lov.	§ 4 nr (1)	
Forvaltningsorganet	Kan i det enkelte tilfelle be om opplysninger som bekrefter avsenders identitet eller fullmakter, eller stille krav om at bestemte sikkerhetstjenester og -produkter skal tas tas i bruk, dersom dette er av betydning for håndtering av henvendelsen.		§ 4 nr (2)	
Forvaltningsorganet	kan bestemme at krav som nevnt i § 4 nr (2) skal gjelde generelt for nærmere angitte typer av henvendelser.	Kravene skal være basert på forvaltningsorganet sikkerhetsstrategi, jf. § 13.	§ 4 nr (3)	

Forvaltningsorganet	Forvaltningsorganet skal gjøre tilgjengelig sikkerhetstjenester og -produkter som oppfyller de krav forvaltningsorganet har stilt i henhold til § 4 nr (2)-(3) eller anvise hvilke løsninger som ellers kan benyttes. Det samme gjelder for sikkerhetstjenester og -produkter som er nødvendige for oppfylle kravene i § 5.		§ 4 nr (4)	
Når et forvaltningsorgan legger til rette for bruk av elektronisk kommunikasjon for mottak av opplysninger som på forvaltningens hånd kan være underlagt taushetsplikt, eller som kan være underlagt krav til sikring etter reglene om behandling av personopplysninger eller tilsvarende regler	Skal risiko for uberettiget innsyn i opplysningene være forebygget på tilfredsstillende måte.		§ 5 nr (1)	
Forvaltningsorgan, som legger til rette for å motta opplysninger som nevnt under § 5 nr (1)	skal på hensiktsmessig måte informere om eventuell risikoer ved elektroniske overføring av slike opplysninger og om hva som er rette elektroniske adresse.		§ 5 nr (2)	

Forvaltningsorganet	skal opplyse generelt om hvordan taushetsbelagte opplysninger og personopplysninger sikres under behandling i forvaltningsorganet.		§ 5 nr (3)	
	Ved kryptering av melding til forvaltningen	skal forvaltningsorganets krypteringsnøkkel eller krypteringsnøkkel til en nærmere angitt enhet ved forvaltningsorganet benyttes. Hvis forvaltningsorganet benytter ekstern databehandler i henhold til personopplysningsloven § 15, kan databehandlers krypteringsnøkkel benyttes hvis det godtgjøres, eller er alminnelig kjent, at databehandleren opptrer på vegne av forvaltningsorganet.	§ 5 nr (4)	
		Kryptering med en enkeltpersons krypteringsnøkkel kan bare benyttes dersom forvaltningsorganet har lagt spesielt til rette for det.	§ 5 nr (5)	
Forvaltningsorganet	skal forebygge risiko for uberettiget innsyn i enkeltvedtak på en tilfredsstillende måte.		§ 8 nr (4)	Konfidensialitet
		Innsyn etter § 10 nr (2) gis bare når det kan oppnås: b) at risiko for uberettiget innsyn i opplysningene eller dokumentene er forebygget på en tilfredsstillende måte	§ 10 nr (3)	

Forvaltningsorgan som benytter elektronisk kommunikasjon	skal ha beskrevet mål og strategi for informasjonssikkerhet virksomheten (sikkerhetsmål og sikkerhetsstrategi)	Sikkerhetsstrategien skal danne grunnlaget for forvaltningsorganet beslutninger om innføring og bruk av sikkerhetstjenester og -produkter på en helhetlig, planlagt, systematisk og dokumentert måte. Sikkerhetsstrategien skal inkludere relevante krav som er fastsatt i annen lov, forskrift eller instruks.	§ 13 nr (1)	
		Sikkerhetsstrategien skal være utarbeidet i henhold til anerkjente prinsipper for informasjonssystemers sikkerhet.	§ 13 nr (2)	
Forvaltningsorganet	I den utstrekning det er relevant skal sikkerhetsstrategien også adressere, og om nødvendig stille krav til bl.a.	I den utstrekning det er relevant skal sikkerhetsstrategien også adressere, og om nødvendig stille krav til bl.a.	§ 13 nr (3)	
	prosedyrer for anskaffelse, bruk, oppbevaring og sikring av signaturfremstillingsdata, passord/PIN-koder og dekrypteringsnøkkel knyttet til personlige sertifikat eller sertifikat for ansatt i forvaltningen, jf. § 15, § 17 og § 20		§ 13 nr (3) bokstav a	Dersom det brukes elektroniske signaturer

	prosedyrer for anskaffelse, bruk, oppbevaring og sikring av signaturfremstillingsdata, passord/PIN-koder og dekrypteringsnøkkel knyttet til virksomhetssertifikat, jf § 14 og § 21		§ 13 nr (3) bokstav b	Dersom det brukes elektroniske signaturer
	prosedyrer for å etablere og opprettholde et sikkert brukermiljø der det benyttes elektroniske signaturer, kryptering eller andre sikkerhetstjenester, jf. § 18.		§ 13 nr (3) bokstav c	
	prosedyrer for varsling og tilbaketrekking av sertifikat og passord/PIN-koder ved mistanke om tap eller misbruk, jf. § 23		§ 13 nr (3) bokstav d	Dersom det brukes elektroniske signaturer
	prosedyrer for kontroll av sertifikater og tilbaketrekkingslister ved mottak av melding utstyrt med elektronisk signatur, herunder krav til hvor oppdatert informasjon om sertifikaters status bør være for de ulike formål sertifikatene benyttes for, jf. § 25		§ 13 nr (3) bokstav e	Dersom det brukes elektroniske signaturer
	prosedyrer for behandling av personopplysninger og taushetsbelagt informasjon, jf. § 5 og § 24, se også personopplysningsloven § 13 og personopplysningsforskriften kapittel. 2.		§ 13 nr (3) bokstav g	

	prosedyrer for sikkerhetskopiering, oppbevaring og deponering av dekrypteringsnøkkel for opplysninger som angår forvaltningsorganet jf. § 22.		§ 13 nr (3) bokstav h	
Et forvaltningsorgan	skal gi sine ansatte anvisning på hvilke sikkerhetstjenester og -produkter de skal benytte under tjeneste for organet, og hvorledes de skal gå frem for å anskaffe nødvendig utstyr og data, herunder signaturfremstillingsdata og dekrypteringsnøkkel med tilhørende sertifikat samt passord og PIN-koder mv		§ 15 nr (1)	
forvaltningsorganet	Ved anskaffelse av utstyr og data som nevnt i § 15 nr (1), plikter forvaltningsorganet å sørge for at den ansatte får informasjon om a) vedkommendes ansvar og plikter i forbindelse med oppbevaring og bruk av signaturfremstillingsdata og dekrypteringsnøkkel med tilhørende sertifikat samt passord og PIN-koder mv, jf. § 20 og § 23		§ 15 nr (2) bokstav a	
forvaltningsorganet	b) restriksjoner på bruk av data som nevnt i bokstav a)		§ 15 nr (2) bokstav b	

forvaltningsorganet	egen og andres mulighet for å trekke tilbake eller suspendere sertifikat		§ 15 nr (2) bokstav c	Dersom det brukes elektroniske signaturer
forvaltningsorganet	sertifikatets ikrafttredelses- og utløpsdato og virkningen av at sertifikatet løper ut eller blir trukket tilbake		§ 15 nr (2) bokstav d	Dersom det brukes elektroniske signaturer
forvaltningsorganet	hvilke opplysninger om den enkelte som vil fremgå av sertifikatet og sertifikatutsteders behandling av personopplysninger, jf. personopplysningsloven § 19, og		§ 15 nr (2) bokstav e	Dersom det brukes elektroniske signaturer
forvaltningsorganet	forvaltningsorganets sikkerhetsstrategi for øvrig, jf. § 13.		§ 15 nr (2) bokstav f	
forvaltningsansatte	Forvaltningsansatte skal følge instruksene arbeidsgiver har fastsatt om bruk og sikring av virksomhetens informasjonssystemer, herunder om kontroll med materiale som skal lastes ned eller installeres på den ansattes arbeidsstasjon, og forvaltningsorganets sikkerhetsstrategi for øvrig, jf. § 13		§ 18	

Forvaltningsorganet	skal sørge for at enhver, i den utstrekning det er nødvendig, får tilsvarende informasjon som nevnt i § 15 og § 17 (3) i forbindelse med anskaffelse av sertifikat eller, hvis det ikke er mulig, ved første gangs bruk av slike tjenester ved kommunikasjon med et forvaltningsorgan.		§ 19	Dersom det brukes elektroniske signaturer
Forvaltningsorganet	Forvaltningsorganet skal på samme måte informere publikum om at håndtering av signaturfremstillingsdata, passord/PIN-koder og dekrypteringsnøkkel skal skje i henhold til § 20 og § 23.		§ 19 siste punktum	Dersom det brukes elektroniske signaturer
Innehaver av signaturfremstillingsdata		Innehaver av signaturfremstillingsdata skal oppbevare og benytte disse på en slik måte at de ikke gjøres tilgjengelige for andre	§ 20 nr (1)	Dersom det brukes elektroniske signaturer. Gir regler for hvordan signaturfremstillingsdata skal sikres
Innehaver av signaturfremstillingsdata		Innehaver skal aldri forlate arbeidsstasjon og lignende uten å sikre at signaturfremstillingsdata ikke er tilgjengelig for andre. Innehaver skal sikre	§ 20 nr (2)	Dersom det brukes elektroniske signaturer. Gir regler for hvordan signaturfremstillingsdata skal sikres
Innehaver av signaturfremstillingsdata		a) at signaturfremstillingsdata fjernes fra arbeidsstasjonen dersom dataene er lagret i smartkort eller i en annen enhet som lett kan fjernes, og	§ 20 nr (2) bokstav a	Dersom det brukes elektroniske signaturer. Gir regler for hvordan signaturfremstillingsdata skal sikres

Innehaver av signaturfremstillingsdata		at den aktuelle arbeidsoperasjonen er avsluttet og eventuelle lagrede eller behandlede signaturfremstillingsdata er deaktivert, eller	§ 20 nr (2) bokstav b	Dersom det brukes elektroniske signaturer. Gir regler for hvordan signaturfremstillingsdata skal sikres
Innehaver av signaturfremstillingsdata		at signaturfremstillingsdata på annen måte er sikret mot misbruk	§ 20 nr (2) bokstav c	Dersom det brukes elektroniske signaturer. Gir regler for hvordan signaturfremstillingsdata skal sikres
Innehaver av signaturfremstillingsdata		skal ikke overlate disse til andre eller gi andre tilgang til dem.	§ 20 nr (3) første punktum	Dersom det brukes elektroniske signaturer. Gir regler for hvordan signaturfremstillingsdata skal sikres
		Skal noen handle på vegne av en annen skal dette skje med fullmektigens egne signaturfremstillingsdata.	§ 20 nr (3) siste punktum	Dersom det brukes elektroniske signaturer. Gir regler for hvordan signaturfremstillingsdata skal sikres
Innehaver av signaturfremstillingsdata		Bestemmelsene om oppbevaring og bruk av signaturfremstillingsdata gjelder tilsvarende for bruk av passord/PIN-koder og lignende og dekrypteringsnøkkel.	§ 20 nr (4)	

Forvaltningsorganet		Ved bruk av virksomhetssertifikat skal forvaltningsorganet sikre at ikke uvedkommende får tilgang til eller kan benytte tilhørende signaturfremstillingsdata. Organet skal også sikre tilfredsstillende kontroll med og registrering av personell og aktiviteter som benytter slike signaturfremstillingsdata. Sikringstiltakene skal skje i henhold til organets sikkerhetsstrategi.	§ 21 nr (1)	Dersom det brukes virksomhetssertifikater. Gir regler for hvordan signaturfremstillingsdata skal sikres.
Forvaltningsorganet		Når flere personer hver for seg skal disponere virksomhetssertifikat, bør hver enkelt disponere eget virksomhetssertifikat med tilhørende signaturfremstillingsdata.	§ 21 nr (2)	Dersom det brukes virksomhetssertifikater. Gir regler for hvordan signaturfremstillingsdata skal sikres.
Forvaltningsorganet		Ved bruk av virksomhetssertifikat skal det være lagt opp rutiner som sikrer at systemet raskt kan settes i drift med nye signaturfremstillingsdata og nytt sertifikat dersom det sertifikatet som er i bruk, blir trukket tilbake eller signaturfremstillingsdata går tapet.	§ 21 nr (3)	Dersom det brukes virksomhetssertifikater. Gir regler for hvordan signaturfremstillingsdata skal sikres.

Forvaltningsorganet		Det skal vurderes om forvaltningsorganet bør være utstyrt med signaturfremstillingsdata og virksomhetssertifikat fra mer enn en sertifikatutsteder.	§ 21 nr (4)	Dersom det brukes virksomhetssertifikater. Gir regler for hvordan signaturfremstillingsdata skal sikres.
Forvaltningsorganet	Signaturfremstillingsdata og dekrypteringsnøkkel skal være sikret mot misbruk i henhold til forvaltningsorganet sikkerhetsstrategi, jf. § 13		§ 21 nr (5)	Dersom det brukes virksomhetssertifikater. Gir regler for at signaturfremstillingsdata og dekrypteringsnøkkel skal sikres.
Forvaltningsorganet	skal sikre at opplysninger og annet materiale som oppbevares av forvaltningsorganet i kryptert form, ikke blir utilgjengelige som følge av at dekrypteringsnøkler går tapt.	Forvaltningsorganet plikter å oppbevare kopi av dekrypteringsnøkler for slikt materiale.	§ 22 nr (1)	
		Prosedyrer for sikkerhetskopiering, oppbevaring, deponering og utlevering av dekrypteringsnøkkel skal følge anerkjente prinsipper og skal fremgå av forvaltningsorganets sikkerhetsstrategi, jf. § 13.	§ 22 nr (2)	

Innehaver av signaturfremstillingsdata		skal straks varsle sertifikatutsteder eller den som ellers er utpekt til å motta varsel, dersom det oppstår mistanke om at signaturfremstillingsdata er tapt, kommet på avveie eller på annen måte blir eller kan bli misbrukt. Det samme gjelder for bruk av passord/PIN-koder o.l. og dekrypteringsnøkkel.	§ 23 nr (1)	Dersom det brukes elektroniske signaturer
Forvaltningsorganet	skal sikre opplysningene under den videre behandling i organet i henhold til de regler som gjelder for de aktuelle opplysningene		§ 24 nr (3)	Gjelder ved mottak av kryptert melding som er blitt dekryptert.
Kongen	kan utpeke et organ som har koordineringsansvar for forvaltningens bruk av sikkerhetstjenester og -produkter ved elektronisk kommunikasjon med og i forvaltningen.		§ 27 nr (1)	Er relevant ved utforming av sikkerhetsmål og sikkerhetsstrategi etter § 13 men gir ikke virksomheten kompetanse
Koordineringsorganet	skal utarbeide krav til sikkerhetstjenester og -produkter som anbefales brukt ved elektronisk kommunikasjon med og i forvaltningen. Koordineringsorganet skal også vurdere om tilgjengelige sikkerhetstjenester eller -produkter tilfredsstiller kravene.		§ 27 nr (2)	Er relevant ved utforming av sikkerhetsmål og sikkerhetsstrategi etter § 13 men gir ikke virksomheten kompetanse

Koordineringsorganet	kan bestemme at det under tjenester for forvaltningsorganer kun skal benyttes sertifikater fra sertifikatutstedere som har inngått rammeavtale om levering av slike tjenester til forvaltningen eller som er anerkjente av koordineringsorganet.		§ 27 nr (3)	Er relevant ved utforming av sikkerhetsmål og sikkerhetsstrategi etter § 13 men gir ikke virksomheten kompetanse
Koordineringsorganet	kan bestemme at det ved elektronisk kommunikasjon med og i forvaltningen bare skal benyttes sertifikater som er oppført på liste publisert i henhold til forskrift 21. november 2005 nr. 1296 om frivillige selvdeklarasjonsordninger for sertifikatutstedere § 11 første ledd.		§ 27 nr (4)	Er relevant ved utforming av sikkerhetsmål og sikkerhetsstrategi etter § 13 men gir ikke virksomheten kompetanse

NR	**Spørsmål ved semistrukturert intervju i kommuner**	**Svar**	**Merknader**
	Hovedspørsmål - Spørsmål med bakgrunn i forskerspørsmål 2a, og 2b - Undersøke faktisk organisering av informasjonssikkerhetsarbeidet (2a) og hva har vært styrende for organiseringen av informasjonssikkerhetsarbeidet (2b)		**Kartlegge faktisk organisering av informasjonssikkerhetsarbeidet og kartlegge hva som har vært styrende for valg av faktisk organisering og om kommunen har brukt regelverk, instrukser, veiledninger, avtaler, modeller, standarder mv.)**
1	**Hvor mange fag- og fellessystemer har kommunen og hvor mange av disse behandler personopplysninger?**		**Spørsmål for å få i gang samtalen og få intervjuobjektet til å prate om ting de har greie på.**
2	**Kan du beskrive disse helt overordnet?**		**Spørsmål for å få i gang samtalen og**

			få intervjuobjektet til å prate om ting de har greie på. Gir også meg ett inntrykk av systemene slik at jeg bedre kan forstå utfordringene med informasjonssikkerhetsarbeidet.
2a	Hvor mange ansatte har kommunen og på hvor mange fysiske steder har kommunens IT-Avdeling ansvar med system eller driftsstøtte?		Gir meg informasjon om omfag og kompleksiteten til oppgavene til IT-avdelingen.
3	**Hvordan vil du beskrive organiseringen av arbeidet med informasjonssikkerhet i kommunen?**		**Hovedspørsmål for å få belyst personelle og prosessuelle krav.**

3a	Hvem har det overordnede ansvaret for å sikre de personopplysningene som kommunen behandler?	.	Personelle krav – Pof § 2-3 første ledd påpeker at den som har den daglige ledelsen for virksomheten har ansvaret for at bestemmelsene i pof kapittel 2 følges. Bør også spør om hvem som kommunen har definert som behandlingsansvarlig.

3b	Er det etablert et sikkerhetsutvalg eller komité som jobber med sikkerhetsfaglige spørsmål i kommunen? I så fall, hvem er disse? Er det andre som har fått spesielle oppgaver knyttet til sikring av IT-systemene?		Personelle krav – Kartlegg mulige delegasjoner av ansvar og myndighet. Jf kommuneloven. Pålagte plikter for den som har det daglige ansvaret etter pol § 18 første ledd bokstav b og pol § 32 første ledd bokstav c.
3c	Er det noen ansatte som har fått helt konkrete definerte oppgaver som er direkte knyttet til sikring av personopplysninger?		Personelle krav – generelt krav til roller i sikkerhetsarbeidet og prosessuelt krav til å etablere en sikkerhetsorganisasjon med klare ansvars- og myndighetsforhold.
3d	Er det noen ansatte som har ansvaret for å gjennomføre kontroll eller revisjon av tiltak for å sikre personopplysninger?		Personelle krav – rollen som sikkerhetsrevisjon og prosessuelt krav; gjennomføre sikkerhetsrevisjon.
3e	I kommunens behandling av personopplysninger, har dere satt ut driften av noen IT-systemer til eksterne firma? I kommunens behandling av personopplysninger,		Personelle krav – aktør - Bruk av databehandler, kommunikasjonspartnere eller leverandører.

	bruker dere underleverandører som samler inn eller lagrer personopplysninger på vegne av kommunen?		
3f	Har dere avtaler eller kontrakter med noen firma som drifter eller vedlikeholder datasystemer som behandler personopplysninger?	.	Personelle krav – aktør – bruk av leverandører.
3g	Er det laget en instruks som sier hvem som skal utføre de ulike oppgavene i sikkerhetsarbeidet?		Personelle krav – definere roller i informasjonssikkerhetsarbeidet. Også et prosessuelt krav, etablere en sikkerhetsorganisasjon med klare ansvars og myndighetsforhold. Se spørsmål nedenfor.

4	**Hva er etter ditt syn de viktigste utfordringene knyttet til organiseringen av sikkerhetsarbeidet?**		**Hovedspørsmål for å få belyst personelle og prosessuelle krav.**

4a	Kan du beskrive kommunens sikkerhetsorganisasjon?		Prosessuelt krav – Sikkerhetsorganisasjon. Koblet til spørsmålet ovenfor der jeg spør om hvilke personer som har oppgaver relatert til sikring av personopplysninger.
4b	Hvor opptatte er kommunens ledelse av informasjonssikkerhet? Hvem blir tatt med på råd når avgjørelser skal tas?		Prosessuelt krav - Valg og prioriteringer i sikkerhetsarbeidet.
4c	Hvordan blir kommunens ansatte involvert i sikkerhetsarbeidet? Hvordan blir kommunens ansatte lært opp slik at alle følger interne rutiner?		

5	**Hvilke ting mener du er aller viktigst å huske på å ha med når det gjelder å organisere informasjonssikkerhetsarbeidet?**		**Hovedspørsmål for å få belyst prosessuelle krav**

5a	Har dere laget en sikkerhetsstrategi eller annet type dokument som beskriver valg og prioritering i sikkerhetsarbeidet?		Prosessuelt krav – sikkerhetsstrategi.
5b	Har dere gjennomført en risikovurdering av sikkerheten rundt behandlingen av personopplysninger? Hvem er det som har ansvaret for å gjennomføre disse?		
5c	Hvordan har dere gått frem for å gjennomføre risikovurderingen?		Prosessuelt krav – Noen krav til hva som i hvert fall skal gjennomfører ved gjennomføring av en risikovurdering er gitt i pof § 2-4
5d	Har dere definert kriterier for akseptabel risiko for behandlingen av personopplysninger? I så fall hvem har gjort det og hvem har godkjent disse?		
5e	Her dere gjennomført sikkerhetsrevisjon?		
5f	Hvordan har dere gjennomført denne? Kan dere beskrive eller henvise til et dokument som beskriver fremgangsmåten og resultatet av den siste		Prosessuelt krav – Overordnede krav til hvordan sikkerhetsrevisjon skal gjennomføres jf. Pof § 2-5

	sikkerhetsrevisjonen?		
5g	Har kommunene opplevd sikkerhetshendelser og hva gjorde dere da? Hva gjorde dere når det skjedde og har dere gjort noe i etterkant for å forhindre at det skjer igjen?		Prosessuelt krav – Avvikshåndtering. Krav om at det skal finnes et system for avvikshåndtering og noen overordnede krav til hvordan og hva som skal behandles som avvik.

6	**Hva har vært styrende for kommunens arbeid med hvordan organiseringen av informasjonssikkerhetsarbeidet er gjennomført på?**		**Hovedspørsmål for å få belyst forskerspørsmål 2b. Har kommunen brukt regelverk, instrukser, veiledninger, avtaler, modeller, standarder mv.**

6a	Hvor har kommunen hentet inspirasjon og veiledning ved organiseringen av informasjonssikkerhetsarbeidet?		

6b	Har dere brukt noen veiledninger på området? f.eks veiledninger produsert av Datatilsynet eller andre myndigheter?		
6c	Ved bestilling av tjenester fra leverandører for IT-systemer. Hvordan har kravspesifikasjonen blitt utarbeidet?		
6d	Har leverandører gitt kommunen råd innen sikkerhetsløsninger?		
6e	Har kommunen brukt tekniske standarder eller håndbøker under arbeidet med å bygge opp en sikkerhetsorganisasjon?		
6f	Er det andre faktorer som du antar kan ha påvirket kommunens arbeidet med hensyn på organisering av informasjonssikkerhetsarbeidet?		
6g	Har forhold rundt sikring av personopplysninger eller organiseringen av arbeidet vært tema på noen møter innen kommunens styrende organer?		

7	**Innsamling av dokumenter, instrukser, delegasjonsvedtak etc. til dokumentanalysen**		
	Husk å spørre om kopi av eventuelle instrukser som kommunen har utarbeidet ifm IT-systemene og sikkerheten.		
	Hvis kommunen hadde avtaler med underleverandører om drift eller behandling av personopplysninger må jeg huske å spør om jeg kan få kopier av disse avtalene.		Personelle krav – aktør – bruk av leverandører. Pof § 2-15 fjerde ledd – Ansvars og myndighetsforhold skal beskrives i særskilt avtale.